Delinea

Cloud Suite

Administrator Guide

Version: 2023

Publication Date: 12/31/2024

Cloud Suite Administrator Guide

Version: 2023, Publication Date: 12/31/2024

Table of Contents

Introduction to Cloud Suite and PAS

You can enroll and manage Windows and Linux systems so computer accounts can be used to run services and to check out account passwords that are stored in the Privileged Access Service.

Privileged Access Service

Privileged Access Service includes a privileged identity management service that enables you to manage passwords and account information for systems, domains, databases, services, and secret text strings or files that contain secret information. You have the option to deploy the Privileged Access Service using the cloud-based services or you have the option to deploy the Privileged Access Service on-site in your own network, in a private cloud, or in a public cloud instance you manage. You can deploy Privileged Access Service with passwords managed securely using the Delinea cloud-based platform or on-site deployment, using a key management appliance such as SafeNet KeySecure, or using an infrastructure of your choice, such as an internal firewall-protected network, a private cloud, or a public cloud instance such as Amazon Web Services (AWS).

Cloud-based Delinea cloud-based products and services rely on the connectors you install and configure for your organization. The connector acts as a gateway between your internal network and the Delinea cloud-based services you use.

At least one connector is required if you are connecting Active Directory domains on your internal network to Delinea services hosted on the Internet. In addition, the Privileged Access Service requires one or more connectors to enable the network connections to IT systems. Multiple connectors can be installed to support fail over and load balancing.

Customer-managed—If you are deploying the Privileged Access Service inside of the firewall for your organization, you will install and configure an on-site connector and all of the required infrastructure components and services on a single Windows computer on your internal network. At least one connector is required. You can, however, install additional connectors to support fail-over and load balancing.

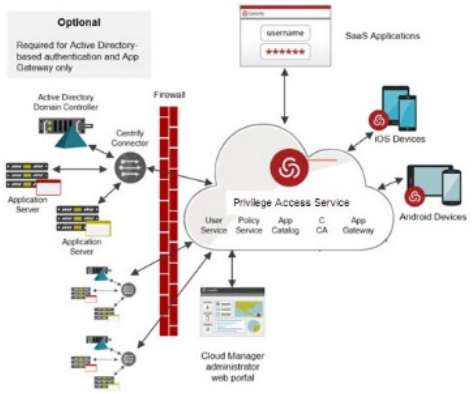
As an on-premise solution that you deploy and manage yourself, Privileged Access Service replicates the infrastructure provided by the Privileged Access Service platform without requiring any access to any cloud based service or any internet connectivity. After you install the basic infrastructure, however, you can choose to host one or more tenants internally on your own network inside of the firewall, or you can use an internet-based third party to host tenants through site to site VPN connections.

After you install Privileged Access Service, you use the Admin Portal to add, manage, and access the systems, domains, databases, services and corresponding accounts you add to the service.

If you are using Active Directory/LDAP to store user accounts, want to continue using it as your primary identity store, and want to continue using the same tools (for example, Active Directory Users and Computers) to manage users and mobile devices, you need to install the Delinea Connector before you can see the Active Directory/LDAP groups when you add users to roles. For more information, see "How to Install a Connector" on page 409. If you use only the Privileged Access Service as your identity store, you do not need to install anything. Everything is configured using Admin Portal. See "Selecting an Identity Repository" on page 221 for more information on the different identity repositories.

Before You Deploy Privileged Access Service

Privileged Access Service is composed of the following services, web portals for administrators and users, and mobile applications users can install on their iOS and Android devices.



- **Policy Service**: A service that provides integrated mobile security management. You configure policies for managing mobile device settings and Privileged Access Service automatically installs the policies in registered devices.

  You can also use the Active Directory Group Policy Management Editor to set mobile device policies. See Selecting a policy service to learn more about your options.

- **Delinea CA**: A certification authority that generates certificates for devices when you use Delinea directory policy service for device policy management. The certificates are automatically generated when you enable wi-fi, VPN, or Exchange ActiveSync policies and select certificates for authentication. The certificates are automatically installed when the user registers the device.

- **App Gateway**: An infrastructure that provides secure access to on-premise web servers. When you use the App Gateway, a VPN is not required. You install the Delinea Connector to use the App Gateway. The App Gateway also provides single sign-on to the web applications.

- **Admin Portal**: The Admin Portal is the web portal you use to configure the Privileged Access Service, deploy web applications, manage users, generate reports, and monitor user activity. If you are using Privileged Access Service for mobile device management, you use Admin Portal to manage the registered devices too.

- **Delinea application**: A free mobile application for Android and iOS devices that users install on their devices to register their devices in the Privileged Access Service. It provides single sign-on to the applications you deploy to them.

  The Delinea application includes a browser that is opened in place of the device's default browser for web applications that require a browser extension to provide single sign-on. This lets users run the same applications they open from their desktop browser on their devices. If the web application does not require the browser extension, the application opens in the user's selected browser.

Privileged Access Service also includes the optional Delinea Connector. This is a software package you install on Windows computers inside your firewall that you can use for any of the following services:

- AD Proxy: You use the Active Directory/LDAP proxy to authenticate users with Active Directory/LDAP accounts for access to the administrator portal. Optionally, this lets you use Active Directory Users and Computers to manage devices and Windows Group Policy Management to manage mobile device policies.
- App Gateway: You use this service to provide secure, remote access to web applications running on internal application servers.
- Active Directory/LDAP Certificate Service (not shown): You can use the default certificate authority instead of the Delinea CA to generate certificates for user authentication. See "How to Select the Policy Service for Device Management" on page 738 for the details.

See How to install a Delinea Connector to download and run the installer.

You install one set of connectors when all of the Privileged Access Service users are in domain trees or forests that have two-way, transitive trust relationships between the domain controllers. If your organization has multiple, independent domain trees or forests, you install a separate sets of connectors for each tree or forest. See "Supporting User Authentication for Multiple Domains" on page 448 for the details.

When you use the connector to authenticate Active Directory users, the installer includes the following extensions:

- **Active Directory Users and Computers console extension** (not shown): A console extension that adds tabs to the mobile device's and user's Active Directory Properties windows with Privileged Access Service information. When you install the console extension, you can use Active Directory Users and Computers to manage devices.

Using Privileged Access Service for Single Sign-On

When you use Privileged Access Service for single sign-on only with the Delinea Directory as your identity store, there is nothing for you to install.

> **Note:** It may be necessary for users to install the Privileged Access Service Browser Extension on their browser. Many popular applications require the browser extension to provide single sign-on.

You can also provide single sign-on to the web applications from the users' devices. In this case, the users need to install the free Delinea application on their devices and register their devices in the Privileged Access Service.

If you want to use your Active Directory/LDAP accounts to authenticate Privileged Access Service users, you install the Delinea Connector and the Active Directory Users and Computers console extension on a Windows computer inside your firewall. Note that Active Directory Users and Computers is for Active Directory deployments only.

Best Practices

Cloud Suite load balances using the public IP address from your egress (public) gateway or the connecting IP address. To help ensure best performance from the web service, your egress gateway should have a sufficiently large enough external IP addresses pool so that requests will be spread across multiple Cloud Suite web nodes. Typically, the IP address pool would have at least 8 unique external IP addresses.

Cloud Clients Scalability Egress

While every environment is different, in general, if using Remote Desktop Protocol or remote SSH, for every 200 Cloud Clients, you should have 2 connectors and each connector should have 2 to 4 external IP addresses. In environments where the Connectors do not handle large amounts of SSH/RDP or LDAP traffic, one Connector

serves as a proxy for 500 Cloud Clients without degradation. Unique IP addresses optimize for best load balancing performance.

Also, routing multiple Cloud Clients through a single gateway can undermine load balancing efforts.

Cloud Connector Scalability Egress

Connectors could serve as a gateway for many systems on your local networks. It is advised that adding more public IP addresses will improve the likelihood that a connector's web traffic is properly distributed across the service. The recommended ratio is 8 public addresses for every 2 connectors.

System Requirements and Supported Browsers

This topic lists browsers and versions tested with the Admin Portal and the Delinea Browser Extension.

Admin Portal Supported Browsers

This version of Privileged Access Service has been tested with the following browsers:

Browser	Version
Internet Explorer	Version 11 on Windows: 2019, 2016, 2012, 2008 servers and Windows 7, and Windows 10. **Note**: Microsoft .NET Framework 4.8 or later is required for Internet Explorer. Additionally, computers must have Microsoft Installer 3.1 or later to install the Delinea Browser Extension
Microsoft Edge Chromium	latest version available at release
Mozilla Firefox	latest version available at release
Google Chrome	latest version available at release

For silent authentication to work correctly, some web browsers need additional configuration (see How to configure browsers for silent authentication) or a browser extension (see How to install the Delinea Browser Extension).

Supported Devices and Systems

The following list of devices and systems are supported in the Privileged Access Service. Delinea has officially tested the system or device versions listed below. However, compatibility is not limited to those versions; versions of the systems or devices not listed may also be compatible.

For Cloud Client supported platforms, see Cloud Client supported platforms.

Operating Systems

- Linux
- Unix
- Windows

Databases

- Microsoft SQL Server (versions 2008R2 and later)
- Oracle (versions 11.2.0.4, 12.1.0.1, 12.1.0.2)
- SAP ASE (version 16.0)

Network Devices and Appliances

- Check Point Gaia (versions R77.30, R80.10)
- Cisco AsyncOS (versions v10 and v11)
- Cisco IOS (versions IOS 12.1/IOS 15.0)
- Cisco NX-OS (version NX-OS 6.0)
- F5 Networks BIG-IP (versions v11, v12, v13)
- HP Nonstop OS (J06.19, H06.29)
- IBM i (versions IBM i 7.2, IBM i 7.3)
- Juniper Junos OS (version JunOS 12.3R6.6)
- Palo Alto Networks PAN-OS (versions 7.1, 8.0)
- VMware VMkernel (versions 5.5, 6.0, 6.5 and 6.7)
- Generic SSH

Desktop Apps

Privileged Access Service provides templates for the following Windows applications in the Desktop Apps feature. Privileged Access Service supports any versions of these applications that are compliant with the requirements for Windows Server 2012 R2 / 2016 Remote Desktop Services and RemoteApp. These applications must accept and process the command line strings pre-defined within the Desktop Apps templates. Delinea has officially tested the following versions:

- SQL Server Management Studio (versions 13.0.15600.2, 2016 and 12.0.4522.0, 2012)
- TOAD for Oracle (version 13.0.0.80)
- VMware vSphere Client (version 6.0.0)

> **Note:** VMware vSphere Client supports VMware VMkernel systems with a VMkernel system version below 6.5

> **Tip:** Custom user-defined templates are also available for additional desktop applications.

Built-In Supported Devices

The Delinea Integration Hub with SSH Self Service Resource provides the tools necessary to create, test, and validate numerous custom SSH device plugins, or Resource Profiles, in a self-service model. The SSH device profiles allow for customizations to be made to specific systems and account operations from password management to password reconciliation.

The Delinea Integration Hub: SSH Self-Service Resource Profiles has the following features:

- Ability to add thousands of varying device types that support the SSH protocol.
- Resource profiles for SSH-enabled devices.
- Ability to define custom system profiles leveraging the Expect framework.
- Includes support for Credential Verification, Password Rotation, Password Reconciliation, and Proxy Accounts.
- Delivers an SSH Test Kit for validating functionality.

Tip: If your device does not exist, you can build it yourself as long as the device is reachable by SSH.

Review the Firewall Rules

The following shows you how to configure the firewall rules for inbound communication and domain traffic for a Privileged Access Service deployment—including the ports and protocols used between different components—depend on several factors. For example, different ports might be required to support specific features—such as network discovery and auditing—or for different system types.

Note: For information on network firewall requirements, see "Cloud Suite and Connector Outbound Network Firewall Requirements" on page 453.

Depending on the characteristics of your environment, you might want to review all or part of the port requirements:

- System Discovery Prerequisites
- "Basic Port Requirements" on page 152
- "Port Requirements for IIS Applications Pools" on the next page
- "Connection between All Systems and AD Domain Controllers" on the next page
- "Connection between the Audit Management Server and Audit Store" on page 8
- "Connection between All Audited systems and Audit Collectors" on page 8
- "Connection between All Systems and AD Domain Controllers" on the next page
- "Connection between Connector and Privileged Access Service" on page 9
- "Connection between All Connectors to Linux Systems" on page 9
- "Connection between All Connectors to Windows Systems" on page 9
- "Connection between All AD Domain Controllers to Windows Systems" on page 10
- "Connection between the Connector and the Session Auditing Collector" on page 10
- "Connection between the Connector and Remote Sessions" on page 10

For additional details see the diagram in Management port for password operations. Additionally, for connector firewall details see "Firewall and External IP Address Requirements" on page 453

Basic Port Requirements

Be sure the following ports are open for basic Privileged Access Service operation:

- Port 53 (TCP/UDP) for communication between any service instance and the DNS server.
- Port 443 or 555 (TCP) for secure HTTPS communication between any service instance and the connector.

Port Requirements for IIS Applications Pools

Be sure the following ports are open on the IIS server to allow discovery of IIS application pools and related accounts:

- Port 135 (TCP) for inbound communication with the RPC endpoint mapper program.
- A custom inbound firewall rule to allow communication for the DllHost.exe process on all RPC Dynamic Ports.
- Port 139 (TCP) for file and printer sharing (NB-Session-In) inbound communication if the operating system is Windows Server 2016.

For more information about configuring firewall rules for discovery, see System discovery prerequisites.

Connection between All Systems and AD Domain Controllers

Below, the port requirements for communication towards AD. These rules should be set up inbound to every domain controller and in any firewall existing in between the Delinea Audit Management Server and every UNIX and Linux systems that will be joined to AD using Delinea.

Port	Traffic Direction
LDAP, Port 389 (TCP/UDP)	Inbound communication to every domain controller from all systems.
Global Catalog, Port 3268 (TCP)	Inbound communication to every domain controller from all systems
DNS, Port 53 (TCP/UDP)	Inbound communication to every domain controller from all systems.
Kerberos, Port 88 (TCP)	Inbound communication to every domain controller from all systems.
Kerberos, Port Password 464 (TCP)	Inbound to every domain controller from all systems.
SMB/CIFS, Port 445 (TCP)	Inbound communication to every domain controller from all systems.
Time Service, Port 123 (TCP)	Inbound communication to every domain controller from all systems.
RPC Endpoint Mapper, Port 135 (TCP)	Inbound communication to every domain controller from all systems.

Connection between the Audit Management Server and Audit Store

Below, the port requirements for communication towards the audit store. These rules should be set up inbound to this system to allow SQL communication from the audit management server and audit collectors:

SQL, Port 1433 (TCP) -- Inbound to the Audit Store

Connection between All Audited systems and Audit Collectors

Below, the port requirements for communication towards Audit Collector servers. These rules should be set up inbound to Audit Collector servers to allow audited data transaction collection from every audited systems (Windows, UNIX, and Linux):

Direct Audit, Port 5063 (TCP) -- Inbound to Audit Collector

Connection between All Connectors to AD Domain Controllers

Below, the port requirements for communication towards Active Directory (AD). These rules should be set up inbound to every domain controller and all firewalls that exist in between the Delinea Connectors and AD domain controllers. Be sure the following ports are open:

Port	Traffic Direction
Global Catalog, Port 3268 (TCP)	Inbound communication to every domain controller from the Delinea Connector
LDAP, Port 389 (TCP/UDP)	Inbound communication to every domain controller from the Delinea Connector
Kerberos, Port 88 (TCP)	Inbound communication to every domain controller from the Delinea Connector
Kerberos Password, Port 464	Inbound communication to every domain controller from the Delinea Connector
SMB/CIFS , Port 445 (TCP)	Inbound communication to every domain controller from the Delinea Connector
Time Service, Port 123	Inbound communication to every domain controller from the Delinea Connector
DNS, Port 53 (TCP/UDP)	Inbound communication to every domain controller from the Delinea Connector
RPC Endpoint Mapper, Port 135 (TCP)	Inbound communication to every domain controller from Delinea Connector

Note: If DNS is not AD-integrated, that rule should be relevant to the alternative DNS service.

To support network discovery, auditing, and domain account management, be sure the following ports are open between the connector and the domain controller:

- Port 135 for inbound RPC endpoint mapper connections to enable a connector to join an Active Directory domain.
- Port 49152-65535 (TCP) for inbound RPC endpoint (“TCP Dynamic”) connections to enable a connector to join an Active Directory domain.

Connection between Connector and Privileged Access Service

Below, the port requirements for communication towards Privileged Access Service. These rules should be set up outbound to the cloud tenant or the on-premise Privileged Access Service.

- HTTPS 443 TCP Inbound from Delinea Connector to Privileged Access Service.
- Internal "DirectTcp" 30001 TCP Outbound to Delinea Connector from Privileged Access Service.

Note: Each additional connector must have its own IP address.

Connection between All Connectors to Linux Systems

Below, the port requirements for communication between the connector and Linux or UNIX systems:

Port	Traffic direction
SSH, Port 22 (TCP)	Inbound communication to every UNIX and Linux system from Delinea Connector
HTTPS, Port 443 (TCP)	Outbound communication from every UNIX and Linux system to Delinea Connector
API Proxy, Port 8080 (TCP)	Outbound communication from every UNIX and Linux systems to Delinea Connector

Connection between All Connectors to Windows Systems

Below, the port requirements for communication between the connector and Windows systems:

Port	Traffic direction
RDP, Port 3389 or a custom port (TCP)	Inbound communication to every Windows system from Delinea Connector
RPC Endpoint Mapper, Port 135 (TCP)	Inbound communication to every Windows system from Delinea Connector
RPC Endpoint "TCP Dynamic", Port 49152-65535 (TCP)	Inbound communication to every Windows system from Delinea Connector

Port	Traffic direction
SMB/CIFS, Port 445 (TCP)	Inbound communication to every Windows system from Delinea Connector
WinRM over HTTP, Port 5985 (TCP)	Inbound communication to every Windows system from Delinea Connector
WinRM over HTTPS, Port 5986 (TCP)	Inbound communication to every Windows system from Delinea Connector
API Proxy, Port 8080 (TCP)	Outbound communication from every Windows systems to Delinea Connector

For more information about port requirements, see Port Requirements.

Connection between All AD Domain Controllers to Windows Systems

Below, the port requirements for communication between the domain controller and Windows systems:

- Port 135 (TCP) for inbound RPC endpoint mapper connections to enable the computer to join the Active Directory domain.
- Port 49152-65535 (TCP) for inbound RPC endpoint connections (“TCP Dynamic”) to enable the computer to join the Active Directory domain.

Connection between the Connector and the Session Auditing Collector

Below are the port requirements for communication between the connector and collector auditing service running on Windows:

Port 5063 (TCP) for inbound collector connections.

Note: There are additional ports used by the collector service that are not required to be open for the Privileged Access Service. For more information about port requirements for auditing components, see the *Auditing Administrator’s Guide*.

Connection between the Connector and Remote Sessions

Below are the port requirements for communication between the connector and native local client sessions running on Windows:

- Port 22 (TCP) for inbound connector connections when using a native secure shell (SSH) client for remote access.
- Port 5555 (TCP) for inbound connector connections when using a native remote desktop protocol (RDP) client for remote access.

For more information about using a native local client for remote access, see Selecting user preferences.

Managing Firewall and External IP Address Requirements

All connections to the internet made by Privileged Access Service (including Delinea Connector and mobile management) are outbound in nature. No internet facing ingress ports are required. All outbound connections are made by way of TCP to either port 80 or 443 and should not have any restrictions.

To provide the redundancy and availability of an always available Privileged Access Service, the destination resource, IP address, and host for outbound connections will vary over time amongst thousands of addresses. Additionally, the range of which also changes as new resources are provisioned or removed.

Note: Deep packet inspection filtering of HTTPS or SSL traffic by web proxies or security software may cause connectivity issues with Privileged Access Service. To allow for normal service operation, exclude the ports and addresses discussed below from packet inspection.

Option 1: Whitelist Source

Given the variability of connection targets, the simplest whitelist configuration is typically one where filters are based on the traffic source. Specifically, it relates to configurations where you allow all outbound traffic from the host machine and account running the Delinea Connector and for outbound requests made by iOS, Android, and Mac clients. This whitelist may be scoped at the machine, or machine + account, or machine + account + process level depending on the feature set of the security appliance or process in place.

Option 2: Whitelist Source Ports

You can also use a whitelist configuration where all outbound traffic on ports 80 and 443 is allowed from the host machine and account running the Delinea Connector, as well as outbound requests made by iOS, Android, and Mac clients. This whitelist may be scoped at the machine, or machine + account, or machine + account + process level depending on the feature set of the security appliance or process in place.

Option 3: Whitelist Destination

If destination whitelisting is required, you can whitelist outbound ports or TCP Relay IP ranges.

Port numbers	Resource
443	`\*.my.centrify.net` (if you need to whitelist your tenant URL)
80	`privacy-policy.truste.com`
80	`ocsp.digicert.com`

If whitelisting an entire domain (*.centrify.com) is not acceptable per security policy, then you need to whitelist the TCP Relay IP ranges for your relevant Privileged Access Service tenant region. Refer to https://www.microsoft.com/en-us/download/confirmation.aspx?id=56519 for a list of Microsoft Azure data center IP ranges by region.

Tenants

If your tenant is on third-party servers, then you need to whitelist the IP ranges for your relevant Privileged Access Service tenant region. Download the relevant file that contains the IP address ranges information. For AWS

you can download them from https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html.

Use the table below to find the TCPRelay IP address ranges for each tenant's region:

Region	IP Address Range
US East	3.14.30.0/27 (adding 4 May 2019) 13.58.135.200/29 18.216.13.0/26 34.236.32.192/26 34.236.241.0/29
US West	13.56.112.160/29 13.56.112.192/26 34.215.186.192/26 34.214.243.200/29 35.89.238.96/28 35.89.238.128/27
Canada	35.183.13.0/26 35.182.14.200/29
Europe	18.194.95.128/26 18.194.95.32/29 34.245.82.128/26 34.245.82.72/29
Brazil	18.231.105.192/26 18.231.194.0/29
Australia	13.211.166.128/26 13.211.12.240/29
Singapore	13.250.186.64/26 13.250.186.24/29
London	3.10.127.0/27 3.10.127.64/26 35.176.92.128/26 35.176.92.72/29

For additional information about whitelisting a tenant for use with web proxies and firewalls, see KB-13446.

Registering for Service

To get here, you have most likely already completed a few key steps:

1. You have requested a free trial or subscription to the Privileged Access Service.

   If you did not request a free trial or subscription, fill out the following form to request access to Privileged Access Service:

   https://delinea.com/products/cloud-suite#trial

2. You have registered for a Delinea account with a valid email address and have received an “Activate Your Delinea Account” email followed by a “Your Delinea Account Is Ready - Next Steps” email with your account details.

   Your account details include the user name for an administrative account, a temporary password, and a unique customer identifier.

3. You have logged on using the account name, temporary password, and URL from your email notification.
4. You have set and confirmed a new password to activate your account.

If you have not completed these preliminary steps, stop here and verify that you have received the “Your Delinea Account Is Ready - Next Steps” email and that you can log on using the account information in the email.

Privileged Access Service provides numerous features, functions, and configuration options. The next steps are only intended to get you going with the basic setup for core services. Depending on the additional services you decide to use, additional steps might be required to complete your initial configuration.

For the core services, you need to know how to add roles and users to the directory service, whether you need to install a connector, and whether additional steps are necessary for the services you are deploying.

To get started, you should review the following topics:

- Directory service users and roles
- Adding roles
- Adding Privileged Access Service users
- Assigning users to roles
- Determining whether you need a connector
- Preparing to deploy infrastructure services
- "Next Steps" below

Next Steps

Depending on the services you choose to deploy, some additional planning or configuration might be required. For example, if you are using the service with an external identity store, to enable single sign-on for applications, or to support mobile device management, you might need to perform a few additional steps to complete the initial configuration for those features.

Depending on the services are deploying, you might find the following topics helpful to getting started with Privileged Access Service:

- How to install a Delinea Connector
- Creating policy sets and policy assignments
- How to register devices

- How to define authentication requirements
- Applications
- How to configure user self-service options

Why Managing Privileged Accounts is Important

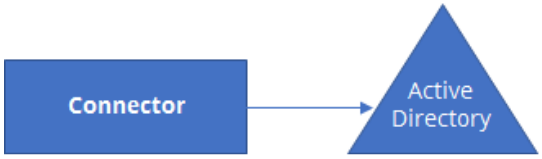
There are several key reasons your organization can benefit from using Privileged Access Service to manage privileged accounts and access to systems, domains, and databases. For example, by using the Privileged Access Service to manage privileged accounts and access to servers, you can:

- Provide access to administrative operations without sharing privileged account passwords.
- Log all password checkout, check-in, and reset activity.
- Change the password stored automatically after a viewed or copied password is checked in to prevent reuse.
- Enforce password complexity by generating passwords that cannot be guessed and that only the service knows.
- Improve your overall operational security by limiting access to accounts with administrative privileges.

Ports for Communication between Components

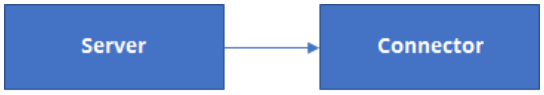
As discussed in "Review the Firewall Rules" on page 6, there are ports required for connections between components. The following summarizes the ports that must be open for **inbound communication** to manage Privileged Access Service's.

Connector to Active Directory Ports (Inbound)



- Global Catalog: 3268
- LDAP: 389
- Kerberos: 88
- Kerberos Password: 464
- SMB/CIFS: 445 for password management
- Time Service: 123
- RPC Endpoint Mapper: 135 (allows the connector to join to an Active Directory domain)
- RPC Endpoint (TCP Dynamic): 49152-65535

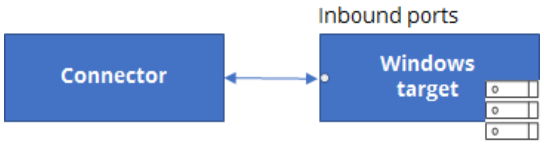
Server to the Connector (Inbound)



The server —- sometimes referred to as the cloud or application server —- handles routing of requests and starting the processes used for management operations.

- HTTPS default port 443
- DirectTCP port 30001

Ports on the Target Windows Server (Inbound)

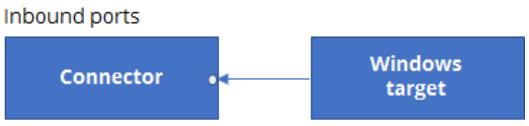


- RDP 3389
- RPC Endpoint Mapper 135
- RPC Endpoint (“TCP Dynamic”) 49152-65535

Ports for Discovery, Testing Connectivity, and Password Management mode

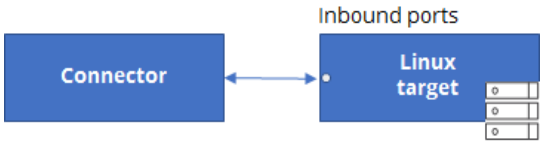
- SMB/CIFS 445
- WinRM over HTTP 5985
- WinRM over HTTPS 5986
- RPC over TCP

Ports on the Connector for the Target Windows Server (Inbound)



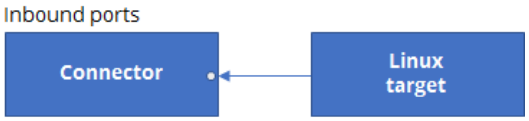
- RDP 3389
- RPC Endpoint Mapper 135
- RDP 5555 (TCP) Connector (inbound) For native RDP

Ports on the Target Linux Server (Inbound)



- SSH 22
- HTTPS 443

Ports on the Connector for the Linux Server (Inbound)



- API Proxy (HTTP proxy) 8080

PAS Firewall Rules and Domain settings for External Integrations

When PAS interacts with your external system there may be additional port requirements.

Note: The outbound 443 port is very likely, with a possibly of other ports, including inbound ports.

Example port recommendations:

Example	Port Recommendations	Protocol
Partner federation / External IDP	Outbound / Inbound 443 for external IDP	HTTPS
SAML app	Outbound / Inbound 443 the application	HTTPS
Customer SMTP server	Port 22	HTTPS

What the Admin Portal Provides

Through the Admin Portal, you can securely store, share, and manage administrative and non-administrative account passwords for target systems, domains, and databases.

By using Privileged Access Service to manage administrative and shared account passwords, you can securely store encrypted passwords and control how frequently they are reset. By adding accounts with managed passwords and only granting specific privileges, you can share common accounts without members of different work groups knowing administrative account passwords.

Using the stored account information, administrators with the proper permissions can log on transparently without providing a password and open remote sessions on target servers and network devices to perform everyday tasks, diagnose problems, or fix issues. In addition, by requiring users to check out and check in stored passwords when

they are not logging on transparently, you can prevent the reuse of shared account passwords for administrative activity.

The Privileged Access Service keeps a record of password check-out, check-in, and session activity, so you always know who had access to which system when. If you also have auditing services installed and have set up an audit installation, you can capture a complete audit trail of what administrators did after starting a remote session on a targeted system. For information about how to create an audit installation to capture and replay session activity, see the *Auditing Administrator's Guide*. For information about configuring auditing for the Privileged Access Service, see Enabling auditing for remote sessions.

Downloading Software

Use the Downloads page to download any of our software components. More details are below.

- Browser extensions - "How to Install the Delinea Browser Extension" on page 850
- Cloud Client for Linux - "Enrolling and Managing Computers Using the Cloud Client for Linux" on page 53
- Cloud Client for Windows - "Installing and Using the Cloud Client for Windows" on page 41
- Cloud Client - "Downloading the Audit Packages for the Cloud Clients" on page 808
- Delinea Connector - "Installing a Delinea Connector" on page 413
- AWS CLI tools - Python and PowerShell command line utilities. The readme files in the download package have instructions for how to use these tools. Also refer to the developer portal for installation information.
- Delinea SSH test kit - "Writing Custom Scripts" on page 634

Deployment Checklists

Privileged Access Service can be deployed in the cloud or on-site in your own network (in a private cloud, or in a public cloud instance you manage). The following checklists provide an overview of the deployment process:

- "Privileged Access Service Deployment Checklist" on page 19 for cloud and on-site deployments.
- "Customer-Managed Privileged Access Service Additional Requirements" below for customer-managed deployments.

The configuration steps that you follow depend on the scope and configuration of your deployment, as well as your assigned role within the Privileged Access Service. Your role assignment in Privileged Access Service controls what you can do and see in the Admin Portal (for details see "Users and Roles" on page 219).

Customer-Managed Privileged Access Service Additional Requirements

See the following details to prepare for installation and deployment of the customer-managed Privileged Access Service. Note that requirements for managed and internal database configurations vary; see "Variations for managed and internal databases."

For additional deployment information, see "Privileged Access Service Deployment Checklist" on page 19.

Getting the Software

- Get a license key from your assigned Sales Engineer.
- Get the unlock code from your assigned Sales Engineer.
- Navigate to the Download Center and use provided codes to download the software.

Servers You Need Before You Install

You will need a total of five Windows 2012 R2 or 2016 servers as follows:

Vault Cluster Servers

Three Windows Servers with the following:

- 16 GB RAM
- 2 CPUs
- 1 fixed IP address per machine.
- Windows Failover Cluster Service installed

Connector Servers

Two Windows Servers with the following:

- 8 GB RAM
- 2 CPUs
- 1 Fixed IP address per machine

IP Addresses You Need Before You Install

- Internal Web IP: vault name requires DNS IP and name.
- Internal WFCS IP: the main server requires a virtual IP.

  Tip: This is the administration access point for the cluster.

Certificates You Need Before You Install

- Web signed certificate IP: This should be a commercial certificate with a built-in root of trust.

  Tip: This is for the URL of the vault.

- Use either a self-signed certificate or use your own custom and/or internal CA.

  Note: If you use your own custom and/or internal CA, you must create a certificate with all DNS names in SAN (subject alternate names) of all clustered nodes.

Database Setup to Prepare Before You Install

Also see "Variations for managed and internal databases" for additional requirements.

- Choose a database name (example: vaultDB).
- Choose a database username (example: vaultDB).

  Note: The database name and database username must be the same.

Security Steps to Take Before You Install

- Plan for a place to store cl.conf file.

  Important: The cl.conf file is a very sensitive file with a security vulnerability, handle accordingly.

Variations for Managed and Internal Databases

Managed database configurations:

- Separate the PostgreSQL cluster
- Install FastDB on an external database

Internal database configuration:

- Requires two ISCSI disks

Privileged Access Service Deployment Checklist

You will need to perform the following initial tasks to:

- Gain access to the Privileged Access Service Admin Portal
- Configure users and roles
- Add and configure resources to be managed by the Privileged Access Service

The initial steps below are included for customer-managed deployments. For additional customer-managed deployment requirements, see "Customer-managed Privileged Access Service additional requirements." If your deployment is a cloud-based deployment, you can start at the "Access the Admin Portal" on page 22 step.

Customer-Managed Steps

The deployment steps in this section apply to you only if you're doing a customer-managed deployment.

Prepare the Virtual Machines

Deployment Step	Configuration location:	Detailed Instructions:
- Join primary server node and secondary server nodes to the domain: - Download primary server and secondary server and import into VMWare. On both systems, join your domain using the system properties or with an administrative PowerShell window. - Install the Windows Failover Clustering feature on both nodes (with Server Manager or using PowerShell).		"Deploying Customer-Managed (On-Premises) PAS" on page 219

Configure a Shared Virtual Disc Host

Deployment Step	Configuration location:	Detailed Instructions:
Note: The following steps are not needed if you are using a customer-managed PostgreSQL database. Make sure the database is configured to be reachable by DNS and have the database user configured.		
- Install and configure the required services. - Configure iSCSI disks and target.	Server Manager > Local Server > File and Storage Services > iSCSI.	"Deploying Customer-Managed (On-Premises) PAS" on page 219
- Configure iSCSI Initiators on primary server and secondary server.	Start > Search > Type iSCSI and open iSCSI Initiator.	"Deploying Customer-Managed (On-Premises) PAS" on page 219
- Initialize the Virtual Disks using the Primary Node (primary server).	Administrative Tools > Disk Management.	"Deploying Customer-Managed (On-Premises) PAS" on page 219

Install Privileged Access Service

Deployment Step	Configuration location:	Detailed Instructions:
- Establish temporary name resolution for primary node. - Install Privileged Access Service on the primary node. - Primary Node verification and hosts file cleanup. - Install Privileged Access Service on the secondary server.	- On primary server logged in as a privileged domain user. - On primary server logged in as Domain Admin. - Admin Portal > Settings > Network. - On secondary server logged in as a privileged domain user.	"Deploying Customer-Managed (On-Premises) PAS" on page 219

Configure Windows Failover Cluster

Deployment Step	Configuration location:	Detailed Instructions:
- Create and validate the cluster.	Administrative Tools > Failover Cluster Manager > Actions, select Create Cluster, this opens the Failover Cluster Wizard.	"Deploying Customer-Managed (On-Premises) PAS" on page 219
Configure Privilege Service as a clustered application.	Administrative Tools > Failover Cluster Manager > Actions > Configure Role.	"Deploying Customer-Managed (On-Premises) PAS" on page 219

Add Cloud Connectors

Deployment Step	Configuration location:	Detailed Instructions:
- Configure Wizard.	Connector configuration Wizard.	"Deploying Customer-Managed (On-Premises) PAS" on page 219

Test Failover

Deployment Step	Configuration location:	Detailed Instructions:
- Review failover policies.	Vault properties window.	"Deploying Customer-Managed (On-Premises) PAS" on page 219
Conduct failover tests: - Maintenance Mode (drain) - Transfer the role to a different cluster node - Simulate Disk Failure - Simulate Network Failure - Stop cisdb-pgsql Stop IIS Web Service (W3SVC) - Operations: Node recoverability - Operations: Backup - Operations: Upgrade - Operations: Restore - Recover from replicated file		"Deploying Customer-Managed (On-Premises) PAS" on page 219
Test the Privileged Access Service instance. Backup and recovery of Privileged Access Service.		"Deploying Customer-Managed (On-Premises) PAS" on page 219

Access the Admin Portal

Deployment Step	Configuration location:	Detailed Instructions:
Request a free trial or subscription.>**Note**: This step is not required if you are performing a customer-managed deployment.	https://delinea.com/products/cloud-suite#trial	"Registering for Service" on page 12

Deployment Step	Configuration location:	Detailed Instructions:
Register for a Centrify account with a valid email address. You will receive an “Activate Your Centrify Account” email followed by a “Your Centrify Account Is Ready - Next Steps” email with your account details. Your account details include the user name for an administrative account, a temporary password, and a unique customer identifier. >**Note**: This step is not required if you are performing a customer-managed deployment.	Email account	"Registering for Service" on page 12
Log in to the Admin Portal using the account name, temporary password, and URL from the email notification. The account used to log on for the first time is a Centrify Directory account and is automatically made a member of the System Administrator role with all administrative rights.	Admin Portal Login Screen	"Registering for Service" on page 12
Set and confirm the new password to activate your account.	Admin Portal Login Screen	

Install the Connector, Integrate Active Directory or LDAP or Federated Users, and Configure Subnet Mapping

Deployment Step	Configuration location:	Detailed Instructions:
Review Cloud Connector requirements. - Check firewall rules for the connections between the Cloud Connectors to the Privileged Access Service. If you are using Discovery, check firewall rules to determine if Cloud Connector can connect to potential resources via SMB and RPC over TCP.	Online help	"Review the Firewall Rules" on page 6 "Determining Whether You Need a Connector" on page 409 Integrating with Microsoft Azure Active Directory Integrating with Idaptive tenants Integrating with Okta
Select a host computer to install the Cloud Connector.	Network	"Configuring the Connector" on page 408
On the host computer, log in to the Admin Portal and select to add a connector and complete installation. Installing the Cloud Connector integrates your Active Directory/LDAP service with Privileged Access Service. The connector allows you to specify groups whose members can enroll and manage devices. It also monitors Active Directory/LDAP for group policy changes, which it sends to Privileged Access Service to update enrolled devices.	Admin Portal> Settings > Network > Cloud Connector	"How to Install a Connector" on page 409
Map a subnet pattern to a selected set of connectors.	Admin Portal> Settings > Resources > System Subnet Mapping	"Mapping System Subnets to Connectors" on page 760

Customize the Admin Portal (Optional)

Deployment Step	Configuration location:	Detailed Instructions:
Customize settings such as login suffix and tenant URLs.	Admin Portal > Settings > General	"Settings UI fields" on page 360
Configure additional customization such as logos and colors for the Admin Portal.	Admin Portal > Settings > General > Account Customization	"How to Customize the Admin and Login Window" on page 249

Add Corporate IP Ranges

Deployment Step	Configuration location:	Detailed Instructions:
Add IP ranges to identify internal and external networks which can be used to specify authentication requirements.	Admin Portal > Settings > Network > Corporate IP Range > Add	"How to Set Corporate IP Ranges" on page 318

Add Users and Roles

Deployment Step	Configuration location:	Detailed Instructions:
Manually create additional System Administrator accounts in the Centrify Directory. You can add Active Directory users in later steps (after you configure the Cloud Connector). Manually create Centrify Directory user accounts in the Centrify Directory.You can also bulk import Centrify Directory users accounts, see How to Bulk import user accounts.	Admin Portal > Access > Users	"Creating Individual Directory Service Users" on page 222
- Add System Administrator accounts to System Administrator roles. - Add Centrify Directory user accounts to roles. By default, users are added to the Everybody role. You can add additional roles with different Administrative rights to control access over who can do what or which policies should be applied to different groups of users.	Admin Portal > Access > Roles	"Adding Roles" on page 220

Configure Policies

Deployment Step	Configuration location:	Detailed Instructions:
Configure user security for Privileged Access Service, such as password-based authentication. In particular, be sure to configure: - Authentication Policies > Centrify Services - User Security Policies - Devices	Admin Portal > Access > Policies	"Creating Policy Sets and Policy Assignments" on page 719 "Reference Content – Roles" on page 275
Configure multi-factor authentication if applicable: - For MFA with mobile device phone numbers: check that these attributes exist and are provisioned in their directory source (Active Directory, Federation etc.) - For MFA with email: check that email attributes exist and have been provisioned in their directory source (Active Directory, Federation etc.) - For RADIUS for MFA: configure RADIUS - For OATH for MFA: configure OATH	(MFA mobile) Identity store–such as Active Directory or another LDAP-based service. (MFA email) Identity store–such as Active Directory or another LDAP-based service (RADIUS) Access > Policies > User Security Policies > RADIUS Also refer to your RADIUS client documentation for additional configuration procedures and guidelines. (OATH) Access > Policies > User Security Policies > OATH OTP Exact configuration steps are dependent on your OATH method.	"How to Configure MFA for Third-Party Integration" on page 350 "Configuring the Delinea Connector for Use as a RADIUS Server" on page 324 "How to Configure OATH OTP" on page 347
Configure global security settings such as frequency of password rotation, minimum password age, how long passwords can be checked out, and so forth.	Admin Portal > Settings > Resources > Security Settings	"How to Set Authentication Security Options" on page 296

Configure Password Profiles

Deployment Step	Configuration location:	Detailed Instructions:
Customize password profiles for systems, domains, and databases.	Admin Portal > Settings > Resources > Password Profiles	"Configuring Password Profiles" on page 751

Add and Configure Resources

Deployment Step	Configuration location:	Detailed Instructions:
Add resources, such as Systems, Databases, Domains, Accounts, Secrets, SSH keys, Services, that you want managed by the Privileged Access Service using one of the following methods: - Import function (Admin Portal Import function or through PowerShell) - Discovery (for Systems and Accounts only) If you are using Discovery, identify an Active Directory account with local administrator permissions to access resources that will be discovered. - Manually	(Import) Admin Portal > Resources > Systems > Import to download the PowerShell script. (Discovery) Admin Portal > Discovery > Systems and Accounts or Alternate Accounts > Profiles (Manually) Admin Portal > Resources >Systems, Databases, Domains, Accounts, Secrets, SSH keys, or Services	"Importing Systems, Accounts, Domains, and Databases" on page 1189 "Discovering Systems" on page 590 "Adding Systems with the Wizard" on page 519
Configure service settings for the following: - Accounts used to run Windows services or scheduled tasks - IIS application pools - Multiplexed accounts used to rotate the password for service accounts	Admin Portal > Resources > Services	"Managing Services" on page 680

Deployment Step	Configuration location:	Detailed Instructions:
Configure permission access for resources. - Individual (all) - Global (Systems and Accounts) - Sets (all)	(Individual) Admin Portal >Resources > select resource type> Permissions (Global) Admin Portal > Access > Global Account Permissions or Global System Permissions (Sets) Admin Portal > Resources > select resource type> Sets	**Individual** "Setting System-Specific Permissions" on page 560 "Setting Domain-specific Permissions" on page 490 "Setting Database-specific Permissions" on page 664 "Setting Secret, Folder, and Set Permissions" on page 503 "Setting Service-specific Permissions" on page 511 **Global** "Setting Global Account Permissions" on page 750 "Setting Global System Permissions" on page 752 **Sets**: *See Individual references above.*

Configure Web Apps

Deployment Step	Configuration location:	Detailed Instructions:
- Add web applications to the Admin Portal app catalog. - Configure application settings. - Assign roles to the application.	Admin Portal > Apps > Add Web Apps	"Adding Web Applications Using the Admin Portal" on page 836

Configure Desktop Apps

Deployment Step	Configuration location:	Detailed Instructions:
- Add desktop applications to the Admin Portal app catalog. - Configure application settings. - Assign roles to the application.	Admin Portal > Apps > Add Desktop Apps	"Adding Desktop Apps Using the Admin Portal" on page 932

Configure Workflow (Optional)

Deployment Step	Configuration location:	Detailed Instructions:
Configure workflow (request and approval access) for Web applications, desktop applications and accounts. - Configure roles for requestors and approvers - Enable workflow for an application or an account - Add approver *To simplify the process of configuring a "request and approval" workflow, you can enable workflow for all accounts stored in the Privileged Access Service.*	**Applications:** Admin Portal > Web Apps or Desktop Apps > select application > Workflow **Accounts**: Admin Portal > Resources > Accounts > select account > Workflow **Global Account Configuration:** Admin Portal > Settings > Resources > Global Account Workflow	"Managing Application Access Requests" on page 794 "Enabling Request and Approval Workflow" on page 475 "Configuring Global Account Workflow" on page 758

Configure Zone Role Workflow for use with Server Suite (Optional)

Deployment Step	Configuration location:	Detailed Instructions:
- Configure Zone Role Workflow (request and approval access) for Systems and Domains. - Configure roles for requestors and approvers. - Enable Zone Role Workflow for all computers in a domain. - Add approver *Systems must be joined to a zone.*	**Systems:** Admin Portal > Resources > Systems > select system > Zone Role Workflow **Domains:** Admin Portal > Resources > Systems > select system > Zone Role Workflow	"Using Zone Role Workflow" on page 776

Configure the Remote Access Kit

Deployment Step	Configuration location:	Detailed Instructions:
If you require remote access to systems using PuTTY or local RDP, install a local client kit and enable access for individual users.	Admin Portal > Settings > Resources > User Preferences	"Selecting User Preferences" on page 764

Enable Auditing for Remote Sessions

Deployment Step	Configuration location:	Detailed Instructions:
- Create an audit installation and verify that the environment is working. - Enable auditing and specify the installation name for the systems you manage in the Admin Portal. *See the Audit and Monitoring Deployment Checklist for additional details.*	Admin Portal > Settings > Resources > DirectAudit	"Enabling Auditing for Remote Sessions" on page 805

Install Cloud Clients

Deployment Step	Configuration location:	Detailed Instructions:
Install the Cloud Client for Linux or the Cloud Client for Windows to allow computer accounts to run services and to check out account passwords that are stored in the Privileged Access Service.	Admin Portal > Downloads	"Installing and Using the Cloud Client for Windows" on page 41 "Enrolling and Managing Computers Using the Cloud Client for Linux" on page 53

Educate End Users

Deployment Step	Configuration location:	Detailed Instructions:
Educate end users on how to: - Configure a user profile - Register devices - Launch web and desktop apps	(User profile) Click Profile under your user name in the Admin Portal. (Register devices) Click Profile > Devices > Add Device under your user name in the Admin Portal. (Launch Apps) Admin Portal > Apps > Web Apps or Desktop Apps	"Using the Tabs" on page 362 "Launching Applications" on page 376 "Selecting Actions for Desktop Apps" on page 934

Introduction to Clients

You can enroll and manage Windows and Linux systems so computer accounts can be used to run services and to check out account passwords that are stored in the Privileged Access Service.

Introduction to Cloud Clients

Cloud Clients provide organizations with a lightweight, high-performance operating system extension for the capabilities of Privileged Access Service. Cloud Suite is the suite of features included with the use of Cloud Clients.

Cloud Clients also work with zone role workflow for both Windows and Linux systems. For details, see Using zone role workflow.

Cloud Client Features

This section provides some overviews of some of the main capabilities that Delinea PAS and Cloud Clients provide.

About Directory Sources and Identity Brokering

You can connect user and group identities from multiple directory sources, such as the following types of directories:

- Active Directory
- Delinea Directory (users defined in Delinea PAS)
- LDAP
- Google

You can also federate with other directories by way of SAML, such as Entra ID, Okta, and so forth. For details, see "How to Set Up Business Partner Federation" on page 261.

For directory sources other than Delinea Directory, you install Delinea PAS software on a system where the directory source is and then you can make sure that those users and groups have access to your resources that are defined in Delinea PAS. This way, you can set up Delinea PAS as an identity broker for multiple directory sources.

For example, by installing Delinea PAS software in AWS, Azure, Google Cloud or a DMZ, you can provide secure access to those systems for your users and groups across various directory sources without having to extend your network. This approach provides decreased exposure, better security, and more flexibility.

For details, see "Directory Service Users and Roles" on page 221.

About MFA Options for Use with PAS and Server Suite

Delinea PAS and Server Suite can support identity assurance by way of multi-factor authentication using the following mechanisms:

Mechanism	NIST 800-53 Assurance	Portal	Client	Notes	Help
FIDO2 Authenticator	High	Supported	Partially Supported	Provides support for YubiKey, Windows Hello, and other password-less mechanisms	How to enable FIDO2 authentication
3rd Party RADIUS Authentication	High	Supported	Supported	Provides MFA brokering for legacy or RADIUS-enabled mechanisms like SecurID, Symantec VIP, Okta RADIUS, Microsoft MFA RADIUS, and so forth.	For use with the Connector: How to configure Privileged Access Service for RADIUS
Delinea Mobile Authenticator	High	Supported	Supported	Provides Support for the Delinea Mobile Authenticator that includes Push MFA and Conditional Access	Using Mobile Authenticator
OATH OTP Client	Medium	Supported	Supported	Provides support for any OATH-compatible authenticator such as Google Authenticator, Red Hat Authenticator, Yubico Authenticator, and so forth.	How to configure OATH OTP
Text message (SMS) confirmation code	Medium	Supported	Supported	Provides SMS-OTP or SMS-Push (if allowed by carrier) for users that have a mobile number in their profile.	Authentication mechanisms
Security Question	Low	Supported	Supported	Provides support for additional secrets in the form of Security Questions.	Authentication mechanisms

Mechanism	NIST 800-53 Assurance	Portal	Client	Notes	Help
Password	Low	Supported	Supported	Provides support for "what you know" secret password. The password policy (such as length, complexity and expiration) are enforceable in the source directory.	Authentication mechanisms

You can use a combination of authentication mechanisms by creating different authentication profiles. Within each authentication profile, you define which mechanisms to use and which users they're for.

You can stack authentication mechanisms with these authentication profiles; you can apply authentication profiles to different user populations by way of policies (for example, employees can use a password + mobile authenticator compared to how contractors use a password + OATH OTP).

You can also configure your authentication profile with a grace period, where under certain conditions if a user needs to re-authenticate during a specified time frame then they don't have to supply credentials again. The MFA grace period applies only to Active Directory users logging in to a Windows system that is joined to Active Directory. For details about how to set up an authentication profile with a MFA grace period, see To create an authentication profile.

For details about the following topics, see the links below:

- "Directory Service Users and Roles" on page 221
- "Policy Assignments" on page 718
- For additional information about Authentication Assurance Levels, review the latest NIST 800-53 publication such as https://pages.nist.gov/800-63-3/sp800-63b.html.

About Access Control Using Roles and Conditions

After you've installed the Cloud Client on a system, you can use both roles and conditional access rules to control access to that system.

By default, users aren't authorized for access to a system where the client is installed. You explicitly grant the permission to log in to a system by granting the AgentAuth permission for a user or role. You can set up roles to leverage the groups that you've already defined in your directory sources. Also, you use the system's Permissions tab to create, modify, and review the permissions for a specific system. The built-in reports can show you who has access to which systems.

You can also define conditional access rules to grant access based on a variety of factors, such as day of the week, time of day, and so forth.

By using role-based access control and conditional access rules, you can set up a robust set of rules for access control.

For details about the following topics, see the links below:

- "Users and Roles" on page 219
- "Setting System-Specific Permissions" on page 560
- "Managing Reports" on page 1053
- "Creating Authentication Rules" on page 281

About Policy Enforcement

Cloud Clients can enforce a variety of policies, such as required multi-factor authentication mechanisms for users to log in. In addition to MFA, clients can enforce conditional access policies and system policy rules. For example, clients can initiate password reconciliation operations on behalf of the shared account password management capability in Delinea PAS.

For details, see "Creating Policy Sets and Policy Assignments" on page 719.

About Privilege Elevation

Privilege elevation provides a way for users to log in as themselves with limited privilege and then request to elevate their access in order to perform privileged operations. Users can then provide additional MFA credentials to continue and run the privileged commands or applications.

By using privilege elevation, you grant access based on Zero Trust principles and then grant privileged access only when needed for a specific operation.

You can grant privileged access to specific commands or all commands. For more information, see "Working with Privilege Elevation" on page 90 and "Specifying Privilege Elevation Commands and Applications" on page 95.

About Linux Group Mapping

With the Cloud Client for Linux, you can map roles to local Linux groups. You can map a role to either an existing local group or a new local group. If the local group doesn't already exist on the systems, the members of the role will show up as members of the group with the details you specify on the role's Unix Profile page.

When you're either creating a new role or editing an existing role, you specify the Linux local group details on the Role > Unix Profile page.

- **New local Linux groups**: Enter the Unix name (required) and the GID (optional).
- **Existing local Linux groups**: Enter the existing Unix name of the local group and the correct GID for the local group.

In the Unix profile you can specify which set(s) of systems to have your role map to.

A previous version of this feature involved setting roles so that they're visible as groups on Linux systems. For details, see "Setting Group Visibility for Clients" on page 764.

About Windows Local Group Mapping

With the Cloud Client for Windows, you can map local groups in Windows to roles in Delinea PAS.

For example, say you have two security groups:

- groupA@corp.acme.com
- groupB@widgets.com

You can configure those security groups to be members of a role in Delinea PAS, let's call it pas-winadmin.

`groupA & groupB _groups = pas-winadmin role`

You can then map the Delinea PAS role to a local Windows administrator group to grant Windows administrator privileges.

The benefits of mapping Windows groups to Delinea PAS roles are:

- On-demand group membership provisioning

  Your Windows credential provider automatically takes care of the group membership.

- Ease of integration

  Use Delinea PAS as the central, corporate tool and workflow utility to manage group memberships, such as adds, moves, and other changes.

Also, if you have mapped any Delinea Directory accounts or federated accounts to the local "Administrators" group, your users can use those accounts to elevate privileges in a User Account Control credential prompt.

For details, see "Mapping Local Groups" on page 552.

About Shared Account Password Management Utilities

Delinea PAS provides shared account password management capabilities for accounts in supported systems, databases and directories. The key benefit is that if a system, container or program needs to provision (set) retrieve (get) or delete (del) types of shared credentials in the Delinea PAS vault, the client provides the `csetaccount`, `cgetaccount` and `cdelaccount` binaries that facilitate these transactions.

In cases of automation, system-to-system authentication, and elimination of static shared credentials (or passwords) from scripts, the Cloud Clients can facilitate these operations while providing the assurance of a strong root of trust.

For details, see the links below:

- "Retrieving Privileged Account Passwords" on page 61
- "Using Cloud Client Commands" on page 111

About Automation

Cloud Clients have been designed to take advantage of many of the elements of the Delinea PAS, these include:

- OAUTH2 limited scopes for the service users.
- PAS Service Users
- Enrollment Codes
- CLI Tooling
- REST APIs
- Sets

These tools allow for automation in several scenarios.

For details, see the links below:

- Automating password rotation
- "Automating Registration" on page 57

Cloud Client Supported Platforms

Cloud Client software has been optimized to work with public and private cloud workloads for 64-bit Windows Server and 64-bit Linux Distributions and Linux Containers (LXC) listed below. For specific version information, please see the release notes.

64-bit Windows Server

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

64-bit Windows Workstation

- Windows 10
- Windows 11

64-bit Linux Distributions

Debian:

- Debian 9, 10, 11
- Ubuntu 18.04, 20.04

RedHat Linux:

- CentOS 7, 8
- RedHat Linux 7, 8, 9-9.4
- Oracle Linux 7.8
- Amazon Linux

SUSE and SLES:

- SLES 12-SP3, 15-SP1

Rocky Linux:

- Rocky Linux 9-9.4

Alma Linux:

- Alma Linux 8.6

64-bit Linux Container

- Alpine Linux

  For Alpine Linux systems, be aware of the following:

  - Alpine Linux is not designed to call the "create home dir" function; so, that means that users will be able to login but they will not have a home directory like on other Linux platforms.
  - You may need to make sure that UsePAM and ChallengeResponseAuthentication or KbdInteractiveAuthentication are both set to yes in the /etc/ssh/sshd_config files.
  - The NSS service doesn't have an /etc/nsswitch.conf file like on other Linux platforms, so you will need to create the /etc/nsswitch.conf file manually.

ARM Linux Distributions

- RHEL 7.6 and higher

Comparing Cloud Clients to Server Suite Agents

In general, you use Cloud Clients with Delinea PAS on systems that are as follows:

- May or may not be joined to Active Directory
- You create as a virtual instance for a short period of time
- Log in with accounts from alternate directory sources

You use the Server Suite Agents with Server Suite for systems that are as follows:

- Joined to Active Directory
- Where you need the Privilege Elevation service

The following tables compare Cloud Client for Windows and Cloud Client for Linux that you download from the Admin Portal to the agents that come with the software for Server Suite.

The Server Suite Agent for *NIX and Server Suite Agent for Windows come with the software for Server Suite.

Clients and Agents for UNIX and Linux Operating Systems

Category	Server Suite Agent for *NIX	Cloud Client for Linux
Supported Platforms	See the Server Suite release notes, which are available in your download package or online. The latest Server Suite release notes are here.	See "Cloud Suite - Release Notes" on page 1200
Workstation OS Supported	Yes	Yes

Category	Server Suite Agent for *NIX	Cloud Client for Linux
Supported Directory Sources	Active Directory	Active Directory, Delinea Directory, Lightweight Directory Access Protocol, Google Directory. You can also federate with other directories by way of SAML, such as Entra ID, Okta, and so forth. For details, see How to set up business partner federation.
UNIX Identity Management	Auto-generated from Delinea or Apple schemes Server Suite Zones via Delinea Standard, RFC-2307 SFU	You can specify Unix profile information on users and roles, and also do bulk import of Unix profiles. For more information, see Specifying UNIX profile information and Importing bulk Unix profiles.
Authentication	Kerberos with NTLM fallback (clients work directly against Active Directory)	Brokered Authentication using SSL/TLS over REST against platform (clients work via the platform, connector talks to the target source directory)
Identity Assurance (MFA)	Supported via PAS Policy and Authentication Profiles	Supported by way of Delinea PAS Policy and Authentication Profiles
Frameworks	Name Service Switch (NSS) Pluggable Authentication Modules (PAM) Kerberos Protocol	Name Service Switch (NSS) Pluggable Authentication Modules (PAM) REST API
Role-based Access Control	Active Directory with Zone Authorization (DirectAuthorize) applicable to AD users/groups	PAS Permissions leveraging (AgentAuth) applicable to any supported directory users/groups.
Audit Trail	CEF-formated by way of Syslog	Not CEF-formatted by way of the Event Table
Session Capture and Replay	Supported. Requires Audit and Monitoring Service Requires Active Directory for Collector, Management, Database and Consoles	Supported. Requires the following: Audit and Monitoring Service 19.9 and up and PAS version 19.6 HF5. Requires Active Directory for Collector, Management, Database and Consoles
SAPM Tooling	Binaries for Linux only. Requires Cloud Client for Linux	Supported

Windows Server Operating Systems

Category	Server Suite Agent for Windows	Cloud Client for Windows
Supported Platforms	All Microsoft-supported (64-bit)	Windows Server 2012 R2 (64-bit) Windows Server 2016 (64-bit) Windows Server 2019 (64-bit)
Workstation OS Supported	Yes	Yes
Supported Directory Sources	Active Directory	Active Directory, Delinea Directory, Lightweight Directory Access Protocol, Google Directory. You can also federate with other directories by way of SAML, such as Entra ID, Okta, and so forth. For details, see How to set up business partner federation.
Local Identity Management	Using Active Directory and Server Suite Zones (Release 2020 - September)	Partial (on-demand provisioning and group mapping)
Authentication	Microsoft Built-in.	Delinea-provided brokered Authentication using SSL/TLS over REST against platform (clients work via the platform, connector talks to the target source directory)
Identity Assurance (MFA)	Supported by way of Delinea PAS Policy and Authentication Profiles	Supported by way of Delinea PAS Policy and Authentication Profiles
Frameworks	Microsoft Authorization Manager (RBAC) Delinea Kerberos Extensions (Privilege Elevation) Microsoft Credential Provider	Microsoft Credential Provider
Role-based Access Control	Active Directory with Zone Authorization (DirectAuthorize) applicable to AD users/groups	Delinea PAS Permissions leveraging (AgentAuth) applicable to any supported directory users/groups.
Audit Trail	CEF-formated by way of the Application Event Log	Not CEF-formatted by way of the Event Table

Category	Server Suite Agent for Windows	Cloud Client for Windows
Session Capture and Replay	Supported. Requires Audit and Monitoring Service Requires Active Directory for Collector, Management, Database and Consoles	Supported. Requires: Audit and Monitoring Service 19.9 and up and PAS version 19.6 HF5. Requires Active Directory for Collector, Management, Database and Consoles
SAPM Tooling	Requires Cloud Client for Windows	Supported

Cloud Client Services and Dependencies

Cloud Client installs the cagent daemon during enrollment.

The following are requirements for all Cloud Client Linux installations:

- Pluggable Authentication Module (PAM).
- PERL 5 Runtime (some distributions will require manually installing the package).

Alpine Linux special dependencies:

- bash
- perl
- openssh-server-pam
- musl-nscd
- sudo
- nss-pam-ldapd

The apk package manager should automatically install the above packages when installing Cloud Client but may not automatically start the nscd daemon. If it doesn't, run `service nscd start`.

Enrolling and Managing Computers with Cloud Clients

You can enroll and manage Windows and Linux systems so computer accounts can be used to run services and to check out account passwords that are stored in the Privileged Access Service.

Installing and Using the Cloud Client for Windows

This section includes topics about installing the client and enrolling your system.

Preparing for the Cloud Client for Windows Installation

The following are considerations and best practices to review and/or perform before you install the Cloud Client for Windows:

Login considerations

The following are login considerations when installing and using the Cloud Client for Windows.

- To Remote Desktop Protocol (RDP) into the Privileged Access Service system, do one of the following:
  - use the Delinea PAS portal web RDP, or
  - use the Microsoft workaround available here.
- Network Level Authentication (NLA) has to be turned off to use **Use My Account** or log in with Delinea PAS.
- When the machine with the Cloud Client for Windows installed on it is joined to a different domain, always input the login suffix for the user login.
- Upon installation and enrollment of the Cloud Client for Windows, local users must use a ".\" prefix (for example: ".\Administrator") to log in.
- If installed on a machine with either: a Cloud Client, a Domain Controller, or a Windows agent installed and configured for MFA -- the Cloud Client for Windows will enroll without failure but will not be enabled. If the client is not enabled, the error is saved in the cenroll log.
- If authenticate profile is disabled or set to "Always allowed", you will be asked for a password upon logon.
- When logging in as an active directory (AD) user, you must log in with the AD user password. If you input the password during MFA, it is used for the AD password because you still log in as the AD user, not a mapped local user.
- If you are unable to log in, it may be because the group policy setting doesn't allow members of the Users group to log in locally. Check your group policy setting by navigating to Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment, and review the policies "Allow log on locally" and "Allow log on through Remote Desktop Services."

Here, you can do one of the following:

1. Add a Users group to the group policy setting "Allow log on locally" **or**
2. Create a local group for cloud users and add this group to "Allow log on locally." Additionally, in the web admin portal set up the local group mapping to map all cloud users to this local group.

Using Sample Scripts for AWS and Azure

The following sample scripts illustrate some common use cases for the commands in the client package. For example, there are sample scripts that illustrate how to use the commands in the client package to perform the following tasks:

- "Retrieve and Install the Cloud Client for Windows in Amazon Web Services (AWS)" below
- "Retrieve and Install the Cloud Client for Windows in Microsoft Azure" on page 44

Retrieve and Install the Cloud Client for Windows in Amazon Web Services (AWS)

To retrieve and install the Cloud Client for Windows in AWS, perform the following steps:

1. Place the package in an online location (in your S3 Bucket), reachable by your AWS instance.
2. Set the variable bucketName to the name of your bucket.

3. Replace regCode with your registration code.
4. Replace cloudURL with your Privileged Access Service URL.
5. Optional: set the addressType to your desired: PrivateIP, PublicIP, PrivateDNS or PublicDNS.
6. Optional: set the nameType to your desired: Name Tag, Local Hostname, Public Hostname or InstanceID.

```
# AWS Bucket Name.
$bucketName = "bucket-name"
# Name of package file.
$packageFilename = "package-name.msi"
# Registration code to use.
$regCode = "SOME-REGISTRATION-CODE"
# Tenant URL against which to enroll.
$cloudURL = "https://TENANT.my.centrify.net"
# Optional - select the FQDN Type (PrivateIP, PublicIP, PrivateDNS, PublicDNS). Defaults
to PublicDNS.
$addressType = ''
# Optional - select the Name Type (NameTag, LocalHostname, PublicHostname, InstanceID).
Defaults to LocalHostname.
$nameType = ''
$system_name = Get-EC2InstanceMetadata -Category LocalHostname
$instid = Get-EC2InstanceMetadata -Category InstanceId
$tagname = ((Get-EC2Instance -InstanceId $instid) | Select -ExpandProperty
RunningInstance).tag
Write-Output "Retrieving package..."
New-Item -ItemType Directory -Path C:\Centrify
$file = (Read-S3Object -BucketName $bucketName -Key $packageFilename -File
C:\Centrify\$packageFilename)

# Retrieves the Name to be registered in PAS.

switch ($nameType.ToLower())
{
"nametag"         {$system_name = $tagname.Item(0).Value}
"localhostname"   {$system_name = Get-EC2InstanceMetadata -Category LocalHostname }
"publichostname"  {$system_name = Get-EC2InstanceMetadata -Category PublicHostname }
"instanceid"      {$system_name = $instid }
default {$system_name = Get-EC2InstanceMetadata -Category LocalHostname}
}

# Retrieves the FQDN to be registered in PAS.

switch ($addressType.ToLower())
{
"publicip"   {$ipaddr = Get-EC2InstanceMetadata -Category PublicIPv4 }
"privateip"  {$ipaddr = Get-EC2InstanceMetadata -Category LocalIPv4 }
"publicdns"  {$ipaddr = Get-EC2InstanceMetadata -Category PublicHostname }
"privatedns" {$ipaddr = Get-EC2InstanceMetadata -Category LocalHostname }
default {$ipaddr = Get-EC2InstanceMetadata -Category LocalIpv4 }
}

Write-Output "The system will be enrolled as $system_name with IP/FQDN $ipaddr."
```

```
Write-Output "Installing and Enrolling..."
$DataStamp = get-date -Format yyyyMMddTHHmmss
$logFile = '{0}-{1}.log' -f $file.fullname,$DataStamp
$MSIArguments = @(
"/i"
('"{0}"' -f $file.fullname)
"/qn
"/norestart"
"/L*v"
$logFile
" TENANTURL=$cloudURL"
" ENROLLCODE=$regCode"
" PARAM=""--address=$ipaddr --name=$system_name"""
)
Start-Process "msiexec.exe" -ArgumentList $MSIArguments   -Wait -NoNewWindow
```

Retrieve and Install the Cloud Client for Windows in Microsoft Azure

To retrieve and install the Cloud Client for Windows preview in Microsoft Azure, perform the following steps:

1. Place the package in an online location.
2. Replace the name of the installation package in packageFilename.
3. Replace regCode with your registration code.
4. Replace cloudURL with your Privileged Access Service URL.
5. If using Azure storage accounts, provide the Account Name and Key.
6. Optional: select the type of IP/FQDN you would like to use. Defaults to PrivateIP.

```
# Name of package file
$packageFilename = "PACKAGE-NAME.msi"
# Registration code to use
$regCode = "SOME-REGISTRATION-CODE"
# Tenant URL against which to enroll
$cloudURL = "https://TENANT.my.centrify.net"
# Parameters to retrieve from a storage account (storage account name + secret)
$storageAcct = 'YOUR-STORAGEACCOUNTNAME'
$storageKey = 'Long long string that shall not be embedded in scripts'
# Gathers some Azure Instance data
$meta = Invoke-RestMethod -Headers @{"Metadata"="true"} -URI
http://123.456.789.254/metadata/instance?api-version=2017-08-01 -Method get
$privateIP =  $meta.network.interface.ipv4.ipAddress.privateIPaddress
$publicIP =  $meta.network.interface.ipv4.ipAddress.publicIPaddress
$system_name = $meta.compute.name
# Optional - select the FQDN Type (PrivateIP, PublicIP). Defaults to PrivateIP.
$addressType = ''
Write-Output "Retrieving package..."
New-Item -ItemType Directory -Path C:\Centrify
$StorageContext = New-AzureStorageContext -StorageAccountName $storageAcct -
StorageAccountKey $storageKey
```

```
Get-AzureStorageFileContent -ShareName "share" -Path "cagent.msi" -Context
$StorageContext -Destination "C:\Centrify\$packageFilename"
$file = Get-ChildItem -Path "C:\Centrify\$packageFilename"
# Retrieves the FQDN to be registered in PAS.
switch ($addressType.ToLower())
{
"publicip"   {$ipaddr = $publicIP }
"privateip"  {$ipaddr = $privateIP }
default {$ipaddr = $privateIP }
}

Write-Output "The system will be enrolled as $system_name with IP/FQDN $ipaddr."
Write-Output "Installing and Enrolling..."
$DataStamp = get-date -Format yyyyMMddTHHmmss
$logFile = '{0}-{1}.log' -f $file.fullname,$DataStamp
$MSIArguments = @(
"/i"
('"{0}"' -f $file.fullname)
"/qn"
"/norestart"
"/L*v"
$logFile
" TENANTURL=$cloudURL"
" ENROLLCODE=$regCode"
" PARAM=""--address=$ipaddr --name=$system_name"""
)

Start-Process "msiexec.exe" -ArgumentList $MSIArguments -Wait -NoNewWindow
Write-Output "Enrollment Complete."
```

Downloading and Installing the Cloud Client for Windows

To download the Cloud Client for Windows:

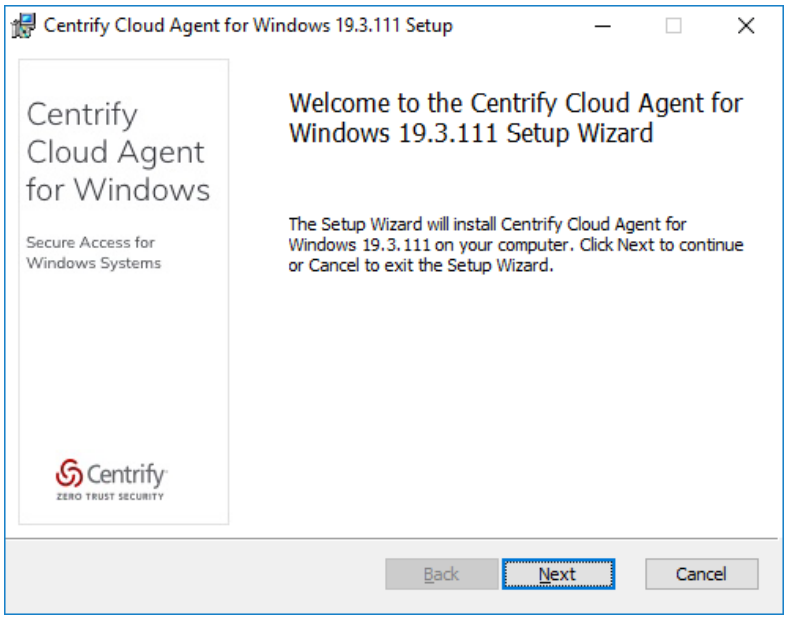
1. Log-in to Admin Portal.
2. Click **Downloads**, select **Cloud Client for Windows** and click **Download**.

> **Note:** When installing the Cloud Client for Windows, irrespective of interactive or silent installation, if you specify parameters, the client is installed and enrolled. If you do not specify parameters, the client is installed successfully but not enrolled.

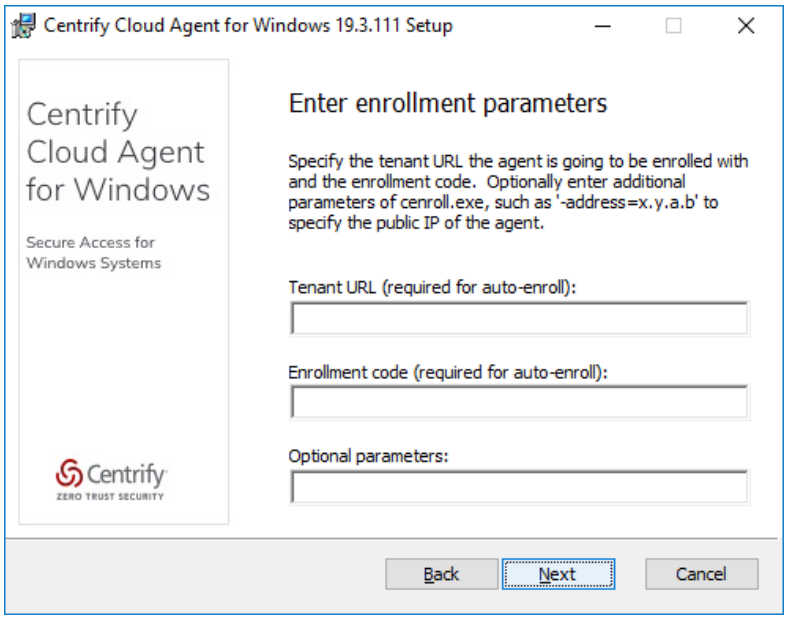
Installing and Enrolling the Cloud Client for Windows Interactively

To install the client interactively:

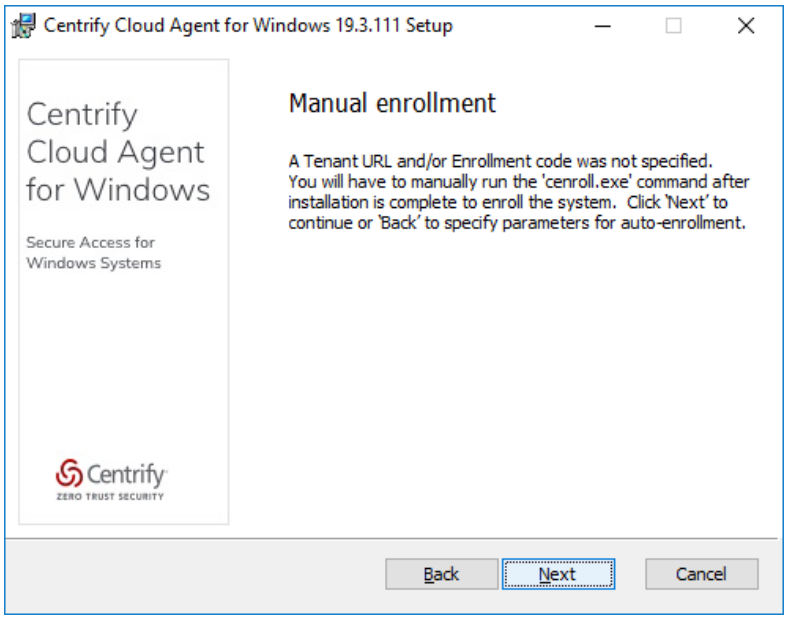
1. Open the downloaded client installer file to start the setup program interactively to a welcome page and click **Next**.



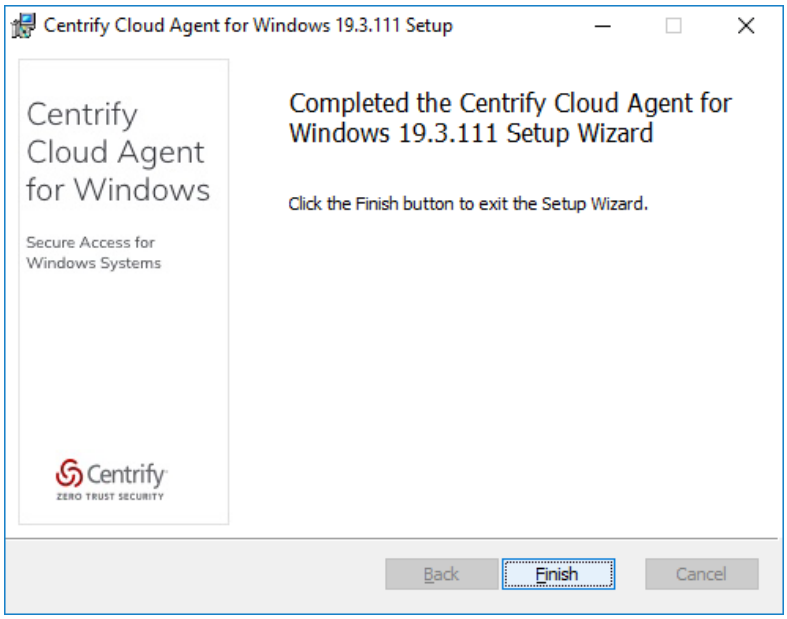
2. At the enrollment parameters screen, enter the enrollment parameters.



Note: If you do not enter enrollment parameters here, the client is installed but not working. The system is not enrolled as no parameters were specified to perform the enrollment . If you don't enter parameters, you will see the following screen and have to run cenroll manually after the installation:

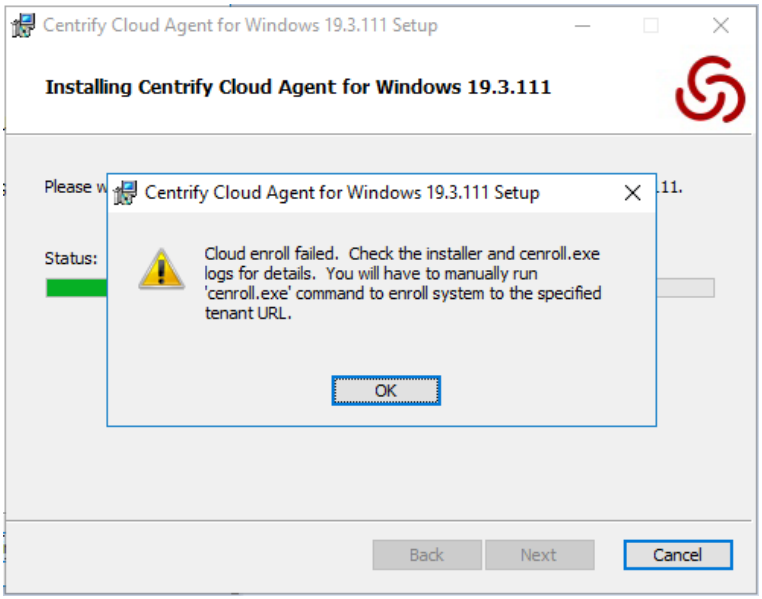


A successful installation screen appears if you have succeeded in one of the following scenarios:



- You entered the correct enrollment parameters and both the installation and enrollment are completed and the client is up and running.
- You did not enter enrollment parameters and installation is complete. The system is not enrolled and you must conclude the enrollment manually after the installation with the command cenroll.

If the installation was successful but the system failed to enroll due to an error (for example, a typo in the enrollment code would prevent the enrollment from completing) you will see the below screen and must manually run cenroll to enroll the system.



Installing and Enrolling the Cloud Client for Windows Silently

To install the program silently use msiexec.exe utility. Refer to msiexec.exe help for complete set of supported options. Enrollment parameters can be passed to the installer via command line using following parameters:

- TENANTURL - the URL of the tenant portal for your organization.
- ENROLLCODE - the code that is generated by the administrator of the tenant's web portal.
- PARAM - any additional parameters that you want to pass to cenroll.exe. any additional parameters that you want to pass to cenroll.exe. For additional options for cenroll, see "cenroll" on page 116.

The following is an example of a silent installation command line you can use:

```
msiexec.exe /q /i cagentinstaller.msi TENANTURL=<url of the tenant> ENROLLCODE=<enrollment
code generated by the tenant>
```

The Cloud Client for Windows replaces the CLI Toolkit, which was available in previous releases. If you downloaded and installed the CLI Toolkit and have scripts that used the commands included in previous releases, you might need to modify the scripts to work with the Cloud Client for Windows. For more information about migrating scripts from the CLI Toolkit to use the commands included in the Cloud Client for Windows package, see "Migrating Scripts from the CLI Toolkit" on page 65.

Troubleshooting the Cloud Client for Windows Installation

This section covers common questions to help you identify and correct problems with the client installation.

- If the service process of Cloud Client for Windows stops running for any reason, the system enters a Rescue Mode. In Rescue Mode, only local administrators can log on to the system.

Understanding Local Group Mapping

With **Local Group Mapping**, you can map a cloud role to a local group on a Windows system. For example, you create a group in Privileged Access Service and call it "local admins" and map it the local group Administrators. Members of the cloud role “local admins” will be added to the local Windows group Administrators when they are logged into the system.

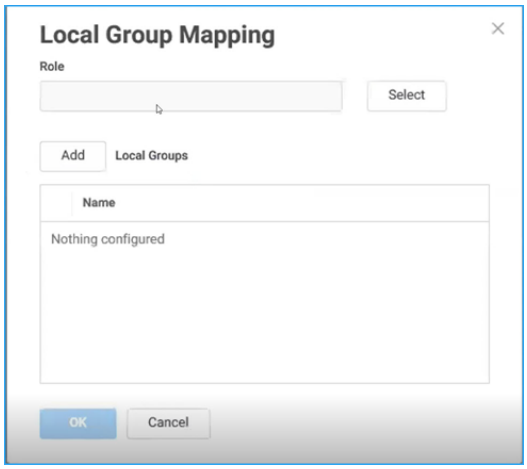
When the user logs out of the system, the service removes the user account from the local group mapping.

Note: If the user has both AgentAuth and Offline Rescue permissions, the local group mapping stays intact after the user logs out. Users with these permissions need to retain local group access between sessions for cases when an offline system needs an administrator to bring it back onlin.

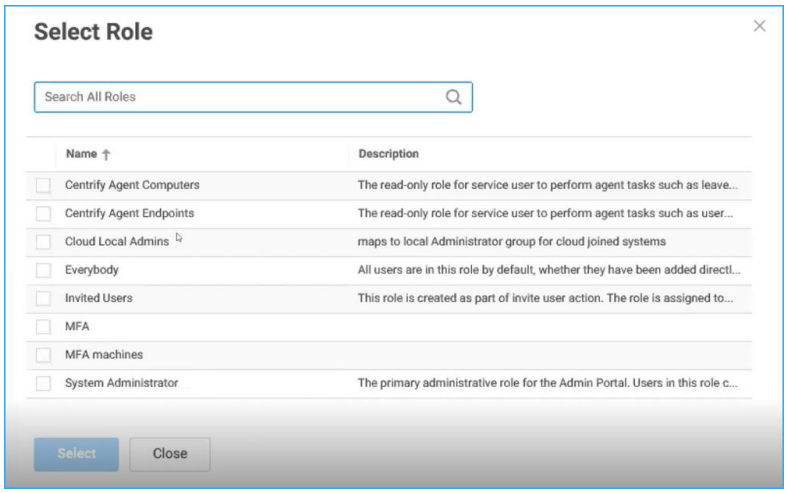
You must have installed the Cloud Client for Windows on the system in order to use **Local Group Mapping**.

To add a group Local Group Mapping:

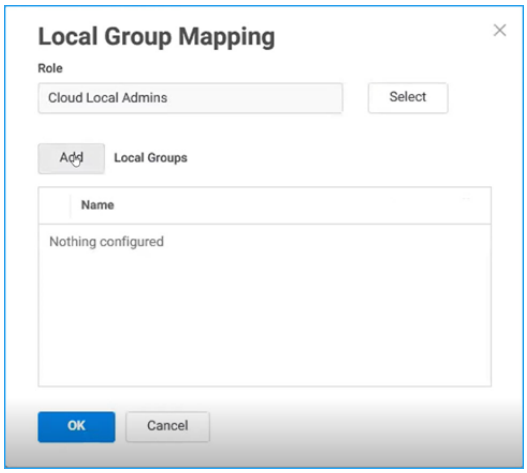
1. Navigate to **Resources** > **Systems**. Choose a system and click **Local Group Mapping** from the left-hand navigation.



2. Select the role you would like to add by clicking **Select** and choose the roles you would like to add:



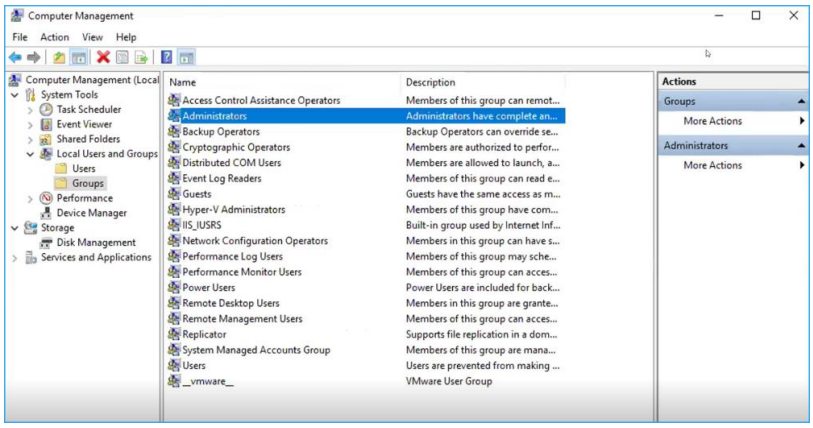
then add the local groups and click **OK** and you will see the group mapping added.



Note: There is no verification on local group naming. If there is a typo in the group naming, the system will look for the group on the local system but may not match due to misspelling and the user will not be added. Additionally, if there is a space in the group name both words must be encased in double quote marks " ".

To verify the group membership, open the Computer Management utility and navigate to **Local Users and Groups**, and *either*:

- Select **Groups**, double-click on the group you're adding user to (Administrators in our example), or
- Select **Users**, double-click on the user and then switch to the **Member Of** tab.



Using Alternative Accounts with Cloud Client for Windows

For systems that are joined to Active Directory and where you have installed the Cloud Client for Windows, you can run an application using Active Directory alternate accounts without having to checkout the password in Delinea PAS.

You'll need to have first discovered the alternate accounts for your users. For details, see Discovering alternative accounts.

Note: The alternate account should not have any MFA settings. If the alternate account does have MFA options assigned, the operation to run the application with that account will fail.

Also, if you're looking for information about enabling alternate account support on systems that have the Server Suite Agent for Windows installed, see Enabling users to run applications with alternate accounts.

To run an application with an alternate account:

1. On a Windows system, right-click the desired application and choose **Run as Administrator**.
2. In the dialog box that opens, select the **Use My Alternate Account** option and click **Yes** to continue.
3. When prompted, enter your Active Directory credentials to authenticate your account and click **Yes** to continue.

   How the authentication profile is configured for your account determines what kind of authentication credentials you need to enter.
4. If you have more than one alternate account, select the desired account to use and click **Yes** to continue.

   If your alternate account has administrative privileges, the application runs under this alternate account (with elevated administrative privileges).

Logging in to Windows with Use My Account

You can log in to an enrolled Windows system with the same account that you use when you log in to the Admin Portal, and you can do this either from the Admin Portal or by using a native application that uses RDP, SSH, SCP, or SFTP.

You can log in to an enrolled Windows system without having to first log in to the Admin Portal by using a vaulted account, manual login, or Use My Account (UMA). For details on logging in with a vaulted or manual account, see Accessing remote systems.

Prerequisites for Logging in to Windows Systems with Use My Account

Before you can use this feature, you need the following:

- Enroll the system. For details, see "Downloading and Installing the Cloud Client for Windows" on page 45.
- Your account needs to have the Agent Auth permission. For details, see "Enabling Client-Based Login" on page 82.
- The target system needs to be using the connector that you log in to. For details, see Mapping system subnets to connectors.

  Note: Be aware that when an Active Directory users logs in with Use My Account, the system prompts them to enter their password so that the user can log in as a domain user on the system.

Accounts and hostnames needed for logging in to Windows systems with Use My Account

Here are the accounts and hostnames that you'll need for this procedure:

- Connector hostname
- Connector port, if you're logging in to the connector in order to connect to another system (jumpbox scenario) By default, the port for RDP connections is 5555 and 22 for SSH connections.

  You can configure the port per connector in Settings > Network > Centrify Connectors > *connector* > SSH-RDP Services > RDP Port. You can also configure the SSH port.
- The target system's hostname (this is the system that you want to log in to). Be sure to use the fully qualified domain name (FQDN).
- Your user name in the Admin Portal, including tenant suffix. For example, joe.user@acme.com.
- The "me" account. This is a local account that the service creates automatically but it's normally hidden from view.

  Note: If you have already configured a local Windows account named "me" you can contact Delinea Technical Support to configure this feature to use a different name for this special, local account.

Whether you connect to a Windows system directly using Remote Desktop Connection, PuTTY, or an FTP client, the process is the same. You connect to the desired system by way of the connector system.

To log in to an enrolled Windows system directly with Remote Desktop Connection:

1. In a new Remote Desktop Connection window, enter the computer hostname and (optionally) the port for the system where the cloud connector is installed.

   For example, if the hostname is win-prod7.acme.com, enter that as the hostname.

   If you're connecting to the system as a way to log in to a networked system (jumpbox scenario), enter the port number. For example, enter win-prod7.acme.com:5555.
2. Enter the user name that you use to log in to the Admin Portal.

   Click **Connect** to continue.
3. When prompted, enter the password for your Admin Portal account.
4. When prompted, enter any additional multi-factor authentication answers.

5. When prompted for the hostname, enter the hostname for the target system.
6. When prompted for the account, enter "me".

   The "me" account tells the service to use your Admin Portal account.

   After the service validates your authentication, it logs you in to the Windows system under your Admin Portal user name.

Enrolling and Managing Computers Using the Cloud Client for Linux

The Cloud Client for Linux is a software package you can install on Linux computers to support agent-based authentication services for all Privileged Access Service users and application to application password management for secure communication between accounts stored in the Privileged Access Service.

By installing the Cloud Client for Linux, computer accounts can be used to run services and to check out account passwords that are stored in the Privileged Access Service. This capability enables you to store and rotate managed passwords for application to application authentication without user intervention and eliminates the need for shared administrative passwords to run services.

Additionally, on registered computers with the agent-based authentication enabled, visible roles become UNIX groups. Each role has a unique name and GID associated with it. Therefore, commands like `getent group <rolename>` executed on registered computers, will return a valid result. If a cloud user is a member of a visible role (visiblerole), commands like `groups <cloudusername>` or `id <cloudusername>` will return a result where the user is considered to be a member of a visible role (visiblerole).

Note: A role does not need to have any members associated with it to be visible on registered computers.

Also see, "Enabling Client-Based Login" on page 82 and "Adding a Role for Client-Based Login" on page 84.

The Cloud Client for Linux is only available for a limited set of supported platforms. If you are managing computers where the client is supported, you can download the client from the Admin Portal, from the Delinea Download Center, or from the Delinea YUM or APT repository.

To download the Cloud Client for Linux

1. Click **Downloads** and review the features available and supported distributions.
2. Click the appropriate link to download the appropriate software package for a supported platform.

For more information about installing and using the Cloud Client for Linux package, see the following topics:

- "Verifying a Signed Package" on the next page
- "Installing the Cloud Client for Linux Package" on the next page
- "Enabling Client-Based Login" on page 82
- "Authorizing Access for the Service User" on page 58
- "Managing Passwords For Services" on page 58
- "Setting Options For Registered Computers" on page 58
- "Customizing Cloud Client Parameters" on page 73
- "Authenticating with a Single-Use SSH Certificate" on page 85

Verifying a Signed Package

You should note that these native packages are signed with a GNU Privacy Guard (GPG) key. If you have not already installed the key on the local computer, you need to import the key to verify the package authenticity before installing the package. Contact Support to get the GPG keys.

After you download the file, you can run a command similar to the following to import the key:

```
rpm --import RPM-GPG-KEY-centrify
```

After you import the key, run the appropriate package manager command to install the package.

For more information about installing and using the Cloud Client for Linux package, see the following topics:

- "Installing the Cloud Client for Linux Package" below
- "Using Cloud Client Commands" on page 111
- "Exploring the Sample Scripts" on the next page

Setting Profile Attributes for Clients

The Cloud Client for Linux is a software package you can install on Linux computers to support password management and authentication services for Privileged Access Service users. To support these features, the client has a **service user** account. The service user requires some additional settings to have a valid profile on the Linux computer where services run or where you are authorizing client-based authentication for access.

To set profile attributes for the client service user:

1. In the Admin Portal > **Settings >Enrollment** to display the settings available for Privileged Access Service.
2. Click **Linux Settings**.
3. Select a default shell from the list of available shells to use for the client service user.
4. Specify the template to use for the home directory for the client service user.
5. Click **Save**.

Installing the Cloud Client for Linux Package

After you download a Cloud Client for Linux, you can use a native package manager to install the commands, man pages, and sample scripts included in the package. For example, if you downloaded the package that supports Red Hat, CentOS, and Oracle distributions of Linux, you would run a command similar to the following on the Linux computer:

```
rpm -Uvh CentrifyCC-rhel6.x86_64.rpm
```

After you install the package using a native package manager, you can find the command line programs and sample scripts in the /usr/bin and /usr/sbin directory. For examples of how you can use the command-line programs in scripts to manage passwords for local or privileged accounts, see the sample scripts included in the /opt/centrify/samples directory.

Note: Perl is required for the Cloud Client for Linux installation on Oracle but is not installed by default. As of Oracle 7.6 this is available as a separate install via: sudo yum install -y perl.

For more information about the Cloud Client package, see the following topics:

- "Using Cloud Client Commands" on page 111
- "Exploring the Sample Scripts" below

Exploring the Sample Scripts

After you install the client package using a native package manager, you can find the command-line programs and sample scripts in the /usr/bin, /usr/sbin, and /opt/centrify/samples directories. The sample scripts in the /opt/centrify/samples directory illustrate some common use-cases for the commands in the client package. For example, there are sample scripts that illustrate how to use the commands in the client package to perform the following tasks:

- Automate the deployment and registration of virtual machines in an Amazon Web Services (AWS) environment (aws_userdata.sh in the /opt/centrify/samples/orchestration directory).
- Write a script to access privileged account passwords stored in the Privileged Access Service (mysql.sh and scp.sh in the /opt/centrify/samples/apppassword directory).
- Write a notification script to automatically add randomly-generated passwords for new local user accounts to the Privileged Access Service (handle_local_accts.cc.sh in the /opt/centrify/samples/localacctmgmt directory).

For more information about copying and modifying the sample scripts, see the README and script file comments in the /opt/centrify/samples directory.

Enrolling a Computer

There are two ways you can register a computer in the Privileged Access Service:

- By using the credentials for a specific user account.
- By using an registration code.

In both cases, you run the `cenroll` command either interactively or in a script to specify registration options, such as the customer-specific URL to use for enrollment, the system-specific policies you want to set, and the features you want to support after registration.

For more information about registering, including examples of the most common registration options, see the following topics:

- "Enrolling with User Credentials" on the next page
- "Using Enrollment Codes" on the next page
- "Enrollment Confirmation" on the next page
- "Automating Registration" on page 57

Note that you can register a computer without specifying a network address by DNS name or IP address. However, you must specify the DNS name or IP address to add local accounts for the system or open secure shell sessions on the system after registration.

For complete information about all of the command-line options available, see the `cenroll` man page.

Enrolling with User Credentials

If you want to register a computer using a specific user name and password, you can run the cenroll command using the `--user` option. The `--user` you specify should be an identity service user in a role with the Linux System Enrollment administrative right. For information about adding roles, members, and administrative rights, see the following topics:

- Creating roles that can create and manage customer's Privileged Access Service
- Admin Portal administrative rights

After you have configured at least one role for registration, you can run a command similar to the following to register a local computer in the Privileged Access Service:

```
 sudo cenroll --tenant abc0123.my.centrify.net
\--username=joe.user@acme.com --features all --owner "Enrollment Admins"
```

The `--owner` option specifies the role with the registration administrative right.

For more information about using enrollment and other commands, see "Using Cloud Client Commands" on page 111.

Using Enrollment Codes

If you want to register a computer using an enrollment code instead of a user name and password, you should verify the following:

- You must be a member of the System Administrator role.
- You must have at least one role with the Linux System Registration administrative right.
- You must generate one or more enrollment codes with the appropriate criteria—such as an expiration date, maximum number of computers that can be registered, or the IP address ranges allowed, if applicable—to be used for registration.

  If you specify IP address restrictions and are connecting to the Privileged Access Service instance through a web proxy server, be sure the IP address for the web proxy server is included in the range allowed.

If you satisfy these prerequisites, you can run the `cenroll` command using the `--code` option. To use an enrollment code, you can run a command similar to the following to register a computer in the Privileged Access Service:

```
sudo cenroll --tenant abc0123.my.centrify.net --code A1BC2345-D6E7-89F0-G123-HIJK4LM5N67P --
features all
```

Enrollment Confirmation

If the cenroll command connects to the Privileged Access Service successfully, you might see confirmation similar to the following in standard output (stdout) or recorded in a log file.

```
cenroll.exe -t abc1234.my.centrify.net -c A1BC2345-D6E7-89F0-G123-HIJK4LM5N67P -f --
features=all
```

```
Enrolling in https://abc1234.my.centrify-qa.net/ ...
Cloud client started.
Enabled features: AgentAuth, AAPM, DMC
Enrollment complete.
```

Automating Registration

You can use the commands included in the client package and registration codes to automate the deployment and removal of virtual machine instances such as Amazon Machine Instances (AMI) in an Amazon Web Services (AWS) cloud environment.

Sample scripts in the client package illustrate how to perform the following tasks when starting a new instance:

- Access the Delinea repository.
- Download and install the client package.
- Run the cenroll program with an registration code and a public IP, private IP, or host name for the network address.
- Configure the secure shell server sshd process.
- Create a shell script for unregistering to be executed when an instance is shut down.

You must modify some configuration details in the sample script -–for example, you must specify your customer-specific URL, registration code, features to enable, and network address type–and run the script as “user data” to register the instance in the Privileged Access Service. After running the script with the appropriate information, the instance will be registered as a system and Delinea identity users can log on to the instance.

For more information, see the README file in the `/usr/share/centrifycc/samples` directory, the README file in the `/usr/share/centrifycc/samples/orchestration` directory, and the comments in the `aws_userdata.sh` sample script.

Verifying Registration

A successful registration updates the Privileged Access Service with new information in several places. After registration, you can verify the new information associated with the computer.

Depending on the features you enable, registration might include all or a subset of the following tasks:

- Add the computer to the Systems tab in the Admin Portal.
- Update the system-specific settings with default values or the settings you specify.
- Update the system-specific policies with default values or the policies you specify.
- Add the service user account for the computer to the Delinea Agent Computers read-only role.

  This role automatically grants the service user the Agent Management (Manage Clients) administrative right to perform agent operations, such as unenroll a computer or set an account password.
- Set system-specific permissions for the service user account for the computer.

Authorizing Access for the Service User

A **service user** is a user account associated with a Cloud Client on a managed Linux computer. The credentials associated with this account are used to authenticate the service when it attempts to perform an operation on a server. Therefore registering a computer and authorizing a service user to access registered computers are key to enabling application-to-application password management.

You should note that a connector is not required to register a computer as an account in the Privileged Access Service. However, you must have a connector installed to support:

- Remote access to computers using secure shell sessions or remote desktop connections.
- The ability to change local account passwords for application-to-application password management (AAPM).

Therefore, if you want to support remote access or enable application-to-application password management, you must have at least one connector installed.

By default, the service user is assigned the Grant, Edit, and Delete permissions on its registered computer and can be used to set passwords for accounts on that computer. For the service user to get passwords for local accounts or for accounts on another computer, however, you must grant the service user Checkout permission. This additional step is required to support application-to-application password management. For more information about setting and retrieving passwords for application-to-application password management, see "Managing Passwords For Services" below.

Setting Options For Registered Computers

You can set a global profile for registered computers and the service accounts associated with the Cloud Client for Linux computers. For example, the service account user you define for an registered computer requires some additional settings to have a valid profile on the Linux computer where services run or where you are authorizing client-based authentication for access.

For information about defining the profile attributes to use for a service account, see "Setting Profile Attributes for Clients" on page 54.

Managing Passwords For Services

You can use the Privileged Access Service to store and retrieve passwords for accounts that are used to access services and in scripts. For example, it is common for organizations to run automated scripts to monitor the operation of computers and devices on the network or to perform administrative tasks without human intervention. In many cases, these scripts require service accounts with permission to perform privileged operations such as automatically archive or remove data from a database. If you have scripts or services that require access to password-protected systems, you might run the risk of having plain text passwords visible.

There are two main password management issues when passwords are required to perform automated or administrative tasks in services or scripts without user interaction:

- Passwords that are hard-coded into scripts are vulnerable to any user who can open the script can see the password displayed as plain text.
- Passwords that are changed periodically to adhere to an organization’s security policies require all scripts to be updated periodically to set the new password.

With Privileged Access Service, you can address both of these issues by doing the following:

- Download the Cloud Client package.
- Identify the computer's service account passwords that need to be stored securely.
- Identify which client computers are allowed to access the stored server account passwords.
- Enroll the server and client computers as systems in the Privileged Access Service.
- Grant the Agent Auth permission to the local and service user accounts that are allowed to access the stored and managed account passwords.
- Modify or create scripts on client computers to replace plain text passwords with calls to the `cgetaccount` command included in the client package.

For more information about managing passwords used to access services and in scripts, see the following topics:

- "Adding Computers as Systems" below
- "Adding Privileged Accounts and Passwords" below
- "Authorizing Password Check Out" on the next page
- "Retrieving Privileged Account Passwords" on page 61
- "Rotating Stored Passwords" on page 63

Adding Computers as Systems

Before you can configure application to application password management, you need to add the computers that will be communicating with each other to the Privileged Access Service. You can complete this step by registering computers in the Privileged Access Service as described in "Enrolling a computer".

If you register a computer and enable the `aapm` feature, the service user account for the computer is automatically added to a Client Management role with administrative rights to use commands such as the `csetaccount`, `cgetaccount`, and `cdelaccount` commands. You can then use these commands in scripts to set, retrieve, and delete manged account passwords. The permissions required are set automatically as part of registration.

Adding Privileged Accounts and Passwords

If you have existing scripts that access protected systems or privileged accounts, you might have existing local account profiles defined in the /etc/passwd file for which you want to manage passwords. If you have an existing local account, you can use the `csetaccount` command interactively or in a script to add the local account and corresponding password to the Privileged Access Service.

For example, you can type the following command to set the password interactively for the local root account and add the password for the account to the Privileged Access Service:

```
csetaccount root
```

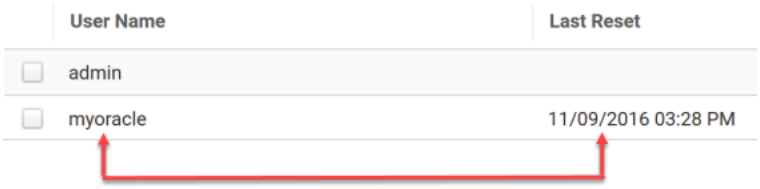
This command prompts you for the account password, then stores the account name and password as an unmanaged password in the Privileged Access Service.

To protect the passwords for accounts with privileged access, you can have the passwords managed by the Privileged Access Service. For example, you might have a local administrative account of myoracle that require access to the root account on a remote computer.

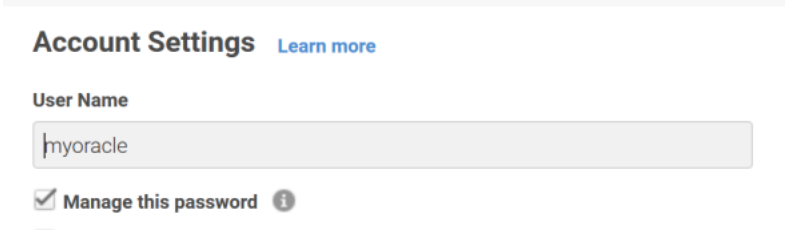
If you wanted the Privileged Access Service to manage the password for the myoracle account, you can add the account by running the-following command interactively or in a script:

```
csetaccoount --managed true myoracle
```

If you type the correct password for the account, the account is added to the Privileged Access Service and a new randomly-generated password is set. You can verify the new account is listed for the system in the Admin Portal.



If you view details for the account, you can confirm the account password is managed by the Privileged Access Service.



Integrating with other Privileged Access Service

If you don't already have local accounts for running services and scripts, you can create them using a program such as useradd or by using Access Manager, `adedit`, or the Access Module for PowerShell if your organization uses additional Privileged Access Service. If you use Privileged Access Service for privilege elevation , you can also define command rights and roles for users who have access to privileged account passwords.

For an example that illustrates how to use client commands in a notification script to set randomly-generated passwords for local accounts, then store those passwords in the Privileged Access Service, see the sample script in the /usr/share/centrifycc/samples/localacctmgmt directory.

Selecting the Password Storage Location

Passwords can be stored securely in the Privileged Access Service or in a key management appliance such as SafeNet KeySecure. However, configuring the password storage location is done separately from adding passwords to the Privileged Access Service. For information about configuring the password storage location, see Managing password storage.

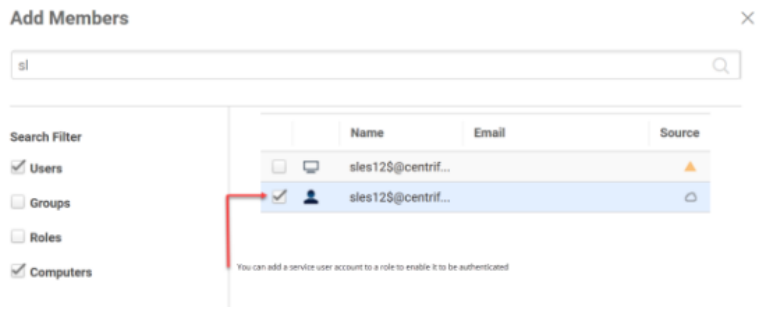
Authorizing Password Check Out

To enable a service user account running a script on a client computer to access the password for a service user account on a server, you must add the client service user account to the list of accounts that have access to the system or to a role with the Agent Auth permission to enable that service user to authenticate using the Cloud Client.

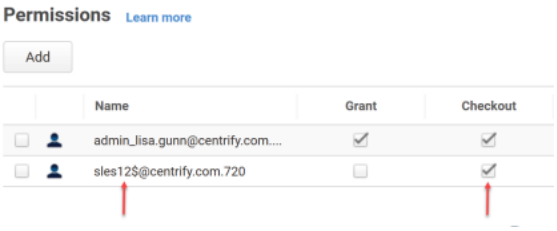
To add the client service user and set the permissions

1. Open the administrative portal from the account name menu.
2. Click **Resources** > **Systems** to select the server system (centos-6) with the account–such as the local root account–the client service user (sles12$) needs to access.
3. Select the local account for the server system.

   For example, select the root account for the centos-6 computer to display the account details.
4. Click **Permissions**, then click **Add** to add the service user that needs to check out the password for the account on the system.
5. Type a search string to locate the client service user account.
6. For example, if the service user for client computer where the script will run is sles12$@cpubs.net, you might type sl to find the account.



7. Select the appropriate account in the results, then click **Add**.
8. Select the **Checkout** permission to allow this account to retrieve the stored password.



9. Click **Save**.

For details about the commandline options for the `cgetaccount` command, type `--help` as a command-line option or display the man page.

Retrieving Privileged Account Passwords

You can use the `cgetaccount` command to check out a password interactively or to retrieve a password silently in a script. For example, you might have a local service account named myoracle with a password that is managed by the Privileged Access Service on the registered computer sles12. To use this account to run a script or open a secure shell, you might need to look up the current password. You can check out the password for the managed account interactively by running a command like this:

```
cgetaccount --lifetime 5 myoracle
```

You are prompted to confirm the checkout and checkout lifetime.

```
Password for account "myoracle" will be checked out. The checkout will be logged and
expire in 5 minutes.
Do you want to continue and display the password? (y/n) y
If you type y to confirm the checkout, the password is displayed as standard output
(stdout). 0
Password for myoracle: ```Fo(\*\~7Ohh()\>UOeO
```

Retrieving a Remote Password Interactively

In a more complex scenario, you might need to check out the password for an account on a remote computer. To illustrate this scenario, the client computer is an registered SuSE Linux computer (sles12) with the local myoracle account that needs access to the password for the root user account on the remote CentOS Linux computer (centos-6).

For example, If you hare configured a command right for the myoracle account, you might retrieve the password for the root account interactively by running a command similar to the following:

If you have configured the sudoers file for the myoracle account, you might retrieve the password for the root account interactively by running commands similar to the following:

```
cgetaccount --lifetime 10 myoracle
```

Because this is a managed account you might need to display and copy the password. You can then use the myoracle account to get the password for the root account

```
su myoracle
```

```
sudo cgetaccount --lifetime 30 CentOS-6.acme.com/root
```

myoracle's password:

In this example, CentOS-6.acme.com is the name of the system as it is stored in the Privileged Access Service. The system name might be the same as or different from the host name or DNS name. You are prompted to confirm the checkout for the root account. If you type y to continue and the password for the root account is also managed in the Privileged Access Service, the current password is displayed and will be changed when the checkout period—in this example 30 minutes—expires.

```
Password for root: 8epM/qL3GtQ[D\>aYe.\*\|
```

Retrieving a Password Using A Command Right

If you have configured a command right for the myoracle account, you might retrieve the password for the root account interactively by running a command similar to the following:

```
su myoracle
```

```
dzdo cgetaccount CentOS-6.cpubs.net/root
```

Retrieving a Password In a Script

You can call the cgetaccount command from within a script to silently retrieve an account password from the Privileged Access Service. By calling the command within a script using a dedicated user account such as the myoracle account, you can prevent other services or scripts from using the client service user account to retrieve a server account password. If you want to use the cgetaccount command to check out, use, and update a managed password from within a script, however, additional steps are necessary to configure the appropriate client and server accounts.

The following example illustrates a shell script that retrieves the password for the myoracle account silently on the sles12 system to perform a backup operation. In this example, the password is checked out for 10 minutes and is displayed as standard output (stdout).

```
\#!/bin/bash

if PASSWORD=\$(cgetaccount -s -t 10 sles12/myoracle); then

.\\run_backup.sh sles12/myoracle \$PASSWORD

else

echo "Failed to get the password for the account."

fi
```

For additional examples of calling the cgetaccount command within a script, see the sample scripts in the /usr/share/centrifycc/samples/apppassword directory.

Rotating Stored Passwords

When you run cgetaccount, you check out the account password for a specified period of time (example: one hour). The account password automatically rotates after that time expires. With `crotatepasswd` you can force the password to rotate so that no one else can use that password and you can do so without waiting for the specified period of time to expire.

The `crotatepasswd` command rotates the password for the specified account from Privileged Access Service. The account can be a system, domain, or database account.

- If you execute `crotatepasswd` specifying the -f option, it ignores any password checkouts and force a password rotation.
- To run the `crotatepasswd` command, you must be logged in as root and the computer where you run `crotatepasswd` must be registered in Privileged Access Service and the Application-to-Application Password Management feature must be enabled.

- As a suggestion, during downtime, have a script execute `crotatepasswd`. If `crotatepasswd` succeeds, have the script then call cgetaccount to get the freshly-rotated password.
- You can force a password rotation for the account "user" on "DOMAIN1" and ignore any password checkouts by running a command such as: `crotatepasswd` -T domain -f DOMAIN1/user.

Enabling MFA for a Cloud Client for Linux

Multi-factor authentication (MFA) is required for all logins to the Cloud Client for Linux (with the exception of local users) .

Note: The login is into registered machines that have a Cloud Client running. Login, used in this context, is the login role.

The **UNIX and Windows Server** login policy dictates how you are authenticated in the system. If you do not have a valid authentication profile set up, you will be denied login. You can disable the MFA requirement for login by setting the parameter pam.mfa.enabled to false in /etc/centrifycc/centrifycc.conf.

To enable MFA for Cloud Client for Linux

1. Enroll the Linux/UNIX machine into Privileged Access Service with agentauth feature permission enabled. At the command prompt on the Linux/UNIX machine, type the following command: sudo cenroll --tenant abc0123.my.centrify.net --user cloudadmin@devserver.sh --features aapm,agentauth -l login -V.

   Note: If you want to log in through MFA, you must have the agent auth permission on the registered machine. This permission can be granted directly, or you can make the user a member of a role with the agent auth permission granted (for example, one specified by a cenroll -l option).

2. Validate your user by running the `getent` command:

```
user@user1:\~\$ getent passwd
genericpasswordgenericpassword:x:5264028:5264028:genericpassword
(Dave@Smith.land):/home/Dave:/bin/bash
```

   Note: If you are enabling MFA for a user, that user must have valid Authentication profile set through the policy and/or role settings in the Admin Portal.

Understanding Cache Objects

A cache object can be either positive or negative as follows:

- **Positive** objects represent queries that previously returned successfully.

For example, if you execute the command `getent passwd foo` and foo refers to an actual user with agent authorization permission on the relevant system, a positive object with the appropriate user details filled in is stored.

- **Negative** objects represent a query that previously returned unsuccessfully (or nothing).

For example, if you execute the command `getent passwd foo`, and foo does not refer to an actual user or refers to a user without agent authorization permission on the relevant system, a negative object entitled "there is no user with Unix name 'foo'" is stored.

Some things to remember:

- Typically only contains partial information (for example, it's not possible to have a negative user with both UID and UNIX Name set, because it's not possible to make such a query at the same time).
- Similarly, if you execute the command `getent group bar`, and bar does not refer to an actual role or to a non-visible role, a negative object stating "there is no role with name 'bar'" is stored.
- When information in a negative object matches that of an about to be stored positive object, the negative object is first removed from the cache.
- Some objects (for example, group membership lists or user group lists) are always positive.

Migrating Scripts from the CLI Toolkit

The Cloud Client replaces the CLI Toolkit, which was available in previous releases from Privileged Access Service and the Delinea Download Center. If you downloaded and installed the CLI Toolkit from a previous release and have scripts that used the commands included in previous package, you might need to modify the scripts to work with the Cloud Client.

Most of the commands included in the client package are the same as the commands included in the CLI Toolkit, but the options supported by each command might be different. In addition, the client package has two new commands —- `cenroll` and `cunenroll` —- that replace the `cjoin` and `cleave` commands in the CLI Toolkit. For details about the options supported for each command, see the man page for that command.

To migrate from the CLI Toolkit to Cloud Client for Linux

1. Run the `cleave` command to unregister the Linux computers where you have installed the CLI toolkit.

   You can upgrade the CLI toolkit to the client package without removing it from the computer.
2. Download and install the appropriate Cloud Client for Linux package as described in "Installing the Cloud Client for Linux Package" on page 54.

   If there are errors, you can review the operation details logged in the `/var/log/centrifycc-install.log` file.
3. Upload a publicly-signed certificate for the Linux computer or configure the Linux computer to trust the Privileged Access Service self-signed certificate.

   The Cloud Client for Linux communicates with the Privileged Access Servicethrough HTTPS, which requires a trusted root certificate to be available. By default, Linux computers will not trust the Privileged Access Service self-signed certificate.
4. Configure optional client settings, such as a web server proxy using parameters in the `/etc/centrifycc/centrifycc.conf` file.
5. Run the `cenroll` command to re-register the Linux computers in the Privileged Access Service after the upgrade by specifying user credentials or an registration code.

   You must specify either `all` or `aapm` for the `--feature` option during registration to use `cgetaccount`, `csetaccount`, and `cdelaccount` commands.

   You can specify an existing system during registration by using the --system-name option to specify the existing system name you want to reuse. However, reusing a system name requires at least one user with sufficient permissions to take over the system. For details about reusing an existing system, see "Taking Ownership of an Existing System" on the next page.
6. Configure permissions after registration.

Setting Permissions for the Service User

After migrating to the Cloud Client for Linux the Active Directory computer account which was used by Delinea CLI Toolkit no longer represents the Linux computer in the Privileged Access Service. Instead, registration creates a new service user account —- such as `rhel\$@centrifydemo.vms` —- to represent the Linux computer in the Privileged Access Service.

The permissions that you previously granted to the Active Directory computer account– such as the permission to check out passwords —- are no longer applicable after migrating to the Cloud Client for Linux. Instead, new permissions need to be granted to the service user. This is especially important for application to application password management scenario to ensure remote computers have the permission to check out service passwords.

Application to Application Password Checkout

To allow service accounts on the sles12 computer to check out an account password from the Privileged Access Service to access accounts on the centos-6 computer, the service user for the sles12 computer must have the Checkout permission for the centos-6 account stored in the Privileged Access Service. For example, the `sles12\$@cpubs.net` account must be able to check out the password for the root user on the centos-6.cpubs.net computer. In addition, the sles12 computer must have an account in the Privileged Access Service that can run root-level commands locally on the sles12 computer to get the password for the remote account.

Grant Permissions

Users must have the Grant permission for a Privileged Access Service account to grant the Checkout permission to other users, groups, or roles. By default, members of the System Administrator role and the user or role who registered a computer are assigned the Grant permission.

Accounts might also be assigned the Grant permission in the following situations:

- If you add the account to the Privileged Access Service by running the Cloud Client `csetaccount` command, the service user account is assigned the Grant permission.
- If you add the account to Privileged Access Service from within the Admin Portal, your logged in user account is assigned the Grant permission.
- If you added the account to Privileged Access Service by running the Delinea CLI toolkit `csetaccount` command, the Active Directory computer account is assigned the Grant permission.

Taking Ownership of an Existing System

As part of the migration from the CLI toolkit to the Cloud Client, you can reuse an existing system name if there is a user with sufficient permissions to take over the ownership of the system. You can migrate a system that was previously added to the Privileged Access Service if you meet one of the following requirements:

- The **owner role** specified when the registration code was generated or using the --owner option at the command-line has Grant, Edit, and Delete permissions for the system.
- The **user credentials** used to register at the command-line specify a user who has Grant, Edit, and Delete permissions for the system.
- The **user credentials** used to register at the command-line specify a user who is a member of the System Administrator role.

How the Linux Client is Different from the CLI Toolkit

The Cloud Client for Linux does not require a connector. However, at least one connector is required to manage the Linux systems and accounts using the Privileged Access Service. The connector also provides a built-in web server proxy to forward HTTPS connection requests to the Privileged Access Service.

The CLI toolkit required Linux computers to be joined to an Active Directory domain and have the adclient process running locally. The Cloud Client for Linux that replaces the CLI toolkit does not require the Linux computer to be joined to a domain or have the adclient process installed.

Logging in to Linux with Use My Account

You can log in to an enrolled Linux system with the same account that you use when you log in to the Admin Portal, and you can do this either from the Admin Portal or by using a native application that uses SSH, SCP, or SFTP.

In particular, you can do this in either of the following scenarios:

- The system has the cloud client installed and the system is enrolled in the platform.
- The system has the Server Suite agent installed and the system is joined to Active Directory and there is a connector installed in the domain.

You can log in to an enrolled Linux system without having to first log in to the Admin Portal by using a vaulted account, manual login, or Use My Account (UMA). For details on logging in with a vaulted or manual account, see Accessing remote systems.

Prerequisites for Logging in to Linux Systems with Use My Account

Before you can use this feature, you need the following:

- Set up the NativeSSH for Use My Account. For details, see "Authenticating with a Single-Use SSH Certificate" on page 85.
- Enable the target system to Use My Account. For details, see "Updating System Settings to Allow Use My Account" on page 88.
- If the Linux system is enrolled, your account needs to have the Agent Auth permission. For details, see "Enabling Client-Based Login" on page 82.

To summarize, depending on your deployment scenario for a Linux system, here's what you'll need:

Requirements	Cloud client (target system is enrolled in the platform)	Server Suite agent (target system is joined to Active Directory)
Permissions	user account in Admin Portal with AgentAuth permission	Active Directory user account
System settings	Target system needs to have Use My Account enabled	Target system needs to have Use My Account enabled
Settings > Authentication > Signing Certificates	a valid signing certificate	a valid signing certificate

If the system is using both the cloud client (enrolled in the platform) and the Server Suite agent, your user account must have AgentAuth permission.

Accounts and Hostnames Needed for Logging in to Linux Systems with Use My Account

Here are the accounts and hostnames that you'll need for this procedure:

- Connector hostname or IP address
- A valid user account:
  - If the system is enrolled in the platform using the cloud client, you can use your user name in the Admin Portal, with tenant suffix. For example, joe.user@acme.com.
  - If the system is joined with Active Directory with the Server Suite agent, you can use your Active Directory user account.
- The target system's hostname (this is the system that you want to log in to)
- The "me" account. This is a local account that the service creates automatically but it's normally hidden from view.

  Note: If you have already configured a local Linux account named "me" you can contact Delinea Technical Support to configure this feature to use a different name for this special, local account.

Connection String Combinations For Logging In To Linux Systems with Use My Account

When specifying which systems to connect to using which accounts, you can use a few different combinations, depending on what you want to do.

In general, here's the format for the connection string:

me@**targetsystem**@**user@domainsuffix**@**connectorsystem**

- **targetsystem**: You can specify a hostname or IP address for this Linux system. For example, target-redhat.acme.com or 172.20.20.250. If specifying a hostname, be sure to use the fully qualified domain name (FQDN).
- **user@domainsuffix**: This is either your Admin Portal user account or your Active Directory user account, depending on your deployment scenario. For example, joe.user@acme.com.
- **connectorsystem**: You specify the Windows system where the cloud connector is installed. For example, connector-win.acme.com.

A connection string doesn't have to contain all these parts. The service will prompt you for anything that is needed that you don't specify in a connection string (such as a password or additional authentication controls).

Logging in to the Target Linux System with Use My Account

You can connect to a Linux system by way of Use My Account (UMA) using SSH, FTP, or SCP, the process is the same. You connect to the desired system by way of the connector system.

To log in to an enrolled Linux system with Use My Account:

- Initiate an SSH, SFTP, or SCP session either from a Windows or UNIX system.

  For example, if you're doing an SSH session from Windows, specify the Windows connector system as the computer name and then specify a connection string that includes your user accounts and the target system details. For example:

  `me@172.20.20.250@joe.user@acme.com` or

  `me@target-redhat.acme.com@joe.user@acme.com`

  If you're doing an SSH session from UNIX or Linux, you can specify some or all of the connection details in the SSH command. For example:

  `ssh me@172.20.20.250@joe.user@acme.com@connector-win.acme.com` or

  `ssh me@target-redhat.acme.com@joe.user@acme.com@connector-win.acme.com`

  You'll be prompted for any details that you didn't provide in the connection string, such as your password or additional authentication credentials.

Using YUM or APT to Install the Client on Linux

To install the Cloud Client for Linux, you can use either the native package manager or repositories such as YUM or APT. This topic covers how to install the client onto systems that use YUM or APT.

- **RedHat, CentOS, Amazon systems**: Use the "Yellowdog Updater, Modified (yum)" tool to update the rpm-redhat repository. For details, see "To Set Up and Configure a RedHat, CentOS, or Amazon Repository" below.
- **Debian or Ubuntu systems**: Use the Advanced Package Tool (APT), apt-get, or Aptitude tools to update the deb repository. For details, see "To Set Up and Configure a Debian or Ubuntu Repository" on page 71.
- **Alpine Linux systems**: For details, see "To Set Up and Configure an Alpine Linux Repository" on page 73.

  Note: The procedures in this section require that you log in to the Delinea Support Portal and go to the Delinea Repo site. On that page, click the link to generate the repo key. You will then specify the repo key in a yum (RHEL, SUSE, and so forth) or APT (Debian, Ubuntu, and so forth) configuration file. There are some examples on the Delinea repo site about how to add the key to your configuration file.

  Note: For additional details about configuring and using SUSE or yum repositories, see the documentation for the distribution of Linux you are using. For additional details about configuring and using APT repositories, see the documentation for the distribution of Debian Linux or Ubuntu you are using.

WARNING: If you specify your repository on the command line, be sure to clean out your command history afterwards. Because the URL for your repository includes the credentials to access it, leaving this information around in command history is not a secure practice.

To Set Up and Configure a RedHat, CentOS, or Amazon Repository

1. Create a /etc/yum.repos.d/centrify-rpm-redhat.repo configuration file to use the official Delinea package repository, and download a RPM-GPG-KEY-centrify key from the Delinea Support Portal.

   You can manually create the configuration file or you can use a setup script to generate the file automatically.

Note: For the baseurl parameter, enter your Delinea repo URL token in place of **<URLtoken>**.

- **To create the repository configuration file manually**

```
# Source: CENTRIFY
# Repository: CENTRIFY / rpm-redhat
# Description: YUM repository for RedHat packages (RPMs)

[centrify-rpm-redhat]
name=centrify-rpm-redhat
baseurl=https://cloudrepo.centrify.com/<URLtoken>/rpm-redhat/rpm/any-distro/any-
version/$basearch
repo_gpgcheck=1
enabled=1
gpgkey=https://downloads.centrify.com/products/RPM-GPG-KEY-centrify
gpgcheck=1
sslverify=1
sslcacert=/etc/pki/tls/certs/ca-bundle.crt
metadata_expire=300
pkg_gpgcheck=1
autorefresh=1
type=rpm-md
```

- **To create the repository configuration file automatically from a script**

```
curl -1sLf 'https://cloudrepo.centrify.com/<URLtoken>/rpm-redhat/cfg/setup/bash.rpm.sh' |
sudo -E bash
```

You should see output that lists out your repository details, such as the following example:

```
# Source: CENTRIFY
# Repository: CENTRIFY / rpm-redhat
# Description: YUM repository for RedHat packages (RPMs)

[centrify-rpm-redhat]
name=centrify-rpm-redhat
baseurl=https://cloudrepo.centrify.com/<URLtoken>/rpm-redhat/rpm/el/6/$basearch
repo_gpgcheck=1
enabled=1
gpgkey=https://cloudrepo.centrify.com/<URLtoken>/rpm-
redhat/cfg/gpg/gpg.BDD3FD95B65ECA48.key
gpgcheck=1
sslverify=1
sslcacert=/etc/pki/tls/certs/ca-bundle.crt
metadata_expire=300
pkg_gpgcheck=1
autorefresh=1
type=rpm-md
```

Note: The gpgkey listed in the output is a public key.

2. Execute the yum info command to verify the repository connection. You should see output similar to the following.

```
# yum info centrifycc
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
2020-11-25 14:36:39,826 [INFO] yum:4208:MainThread @connection.py:905 - Connection built:
host=subscription.rhsm.redhat.com port=443 handler=/subscription auth=identity_cert ca_
dir=/etc/rhsm/ca/ insecure=False
2020-11-25 14:36:39,827 [INFO] yum:4208:MainThread @repolib.py:464 - repos updated: Repo
updates
Total repo updates: 0
Updated
    <NONE>
Added (new)
    <NONE>
Deleted
    <NONE>
This system is not registered with an entitlement server. You can use subscription-manager
to register.
Available Packages
Name        : CentrifyCC
Arch        : x86_64
Version     : 20.6
Release     : 121
Size        : 32 M
Repo        : centrify-rpm-redhat-test/x86_64
Summary     : Cloud Client for Linux
URL         : http://www.centrify.com/
License     : BSD with portions copyright (c) <span class="global-vars.CompanyName mc-
variable">Delinea</span> Corporation 2004-2022 and licensed under <span class="global-
vars.CompanyName mc-variable">Delinea</span> End User License Agreement
Description : RPM to install Cloud Client for Linux on X86_64 platform.
```

3. Install the Cloud Client rpm package.

   ```
   yum install CentrifyCC
   ```

   Note: To uninstall the Cloud Client rpm file, you can use the erase command. For example:

   ```
   yum erase CentrifyCC
   ```

To Set Up and Configure a Debian or Ubuntu Repository

1. Create the repository:

   You can manually create the repository or you can use a setup script to create the repository automatically.

- **To create the Debian or Ubuntu repository configuration file manually**

  a. Update the /etc/apt/sources.list file to include the official Delinea package repository.

  ```
  deb https://cloudrepo.centrify.com/<URLtoken>/deb/deb/debian any-version main
  /etc/apt/sources.list.d/centrify-deb.list
  ```

  b. Import your GPG key and update the repository.

  ```
  # bash -c 'wget -O - https://downloads.centrify.com/products/RPM-GPG-KEY-centrify
  | apt-key add -'
  ```

  c. Comment out the no-debsig line in /etc/dpkg/dpkg.cfg to enable GPG signature validation.

  ```
  # grep no-debsig /etc/dpkg/dpkg.cfg
  # no-debsig
  ```

  d. Clean and update the local archives.

  ```
  # apt-get clean
  # apt-get update
  ```

- **To create the Debian or Ubuntu repository configuration file automatically from a script**

  ```
  curl -1sLf 'https://cloudrepo.centrify.com/<URLtoken>/deb/cfg/setup/bash.deb.sh' |
  sudo -E bash
  ```

  Note: Enter your Delinea repository URL token in place of **<URLtoken>**.

  If you manually created your APT repository, the configuration details are in the /etc/apt/sources.list file. If you used the setup script to create the APT repository, the configuration details are in a separate file such as centrify-deb.list in the /etc/apt/sources.list.d directory.

2. Execute the apt list command to verify the repository connection. You should see output similar to the following.

```
# apt list --all-versions | grep centrify
centrifyda/buster 3.7.0-172 amd64
centrifyda/buster 3.6.1-324 amd64
centrifydc-adbindproxy/buster 5.7.0-217 amd64
centrifydc-adbindproxy/buster 5.6.1-334 amd64
centrifydc-cifsidmap/buster 5.7.0-207 amd64
centrifydc-cifsidmap/buster 5.6.1-330 amd64
centrifydc-curl/buster 5.7.0-207 amd64
centrifydc-curl/buster 5.6.1-330 amd64
centrifydc-ldapproxy/buster 5.7.0-207 amd64
```

```
centrifydc-ldapproxy/buster 5.6.1-330 amd64
centrifydc-nis/buster 5.7.0-207 amd64
centrifydc-nis/buster 5.6.1-330 amd64
centrifydc-openldap/buster 5.7.0-207 amd64
centrifydc-openldap/buster 5.6.1-330 amd64
centrifydc-openssh/buster 8.2p1-5.7.0.207 amd64
centrifydc-openssh/buster 7.9p1-5.6.1.329 amd64
centrifydc-openssl/buster 5.7.0-207 amd64
centrifydc-openssl/buster 5.6.1-330 amd64
centrifydc/buster 5.7.0-207 amd64
centrifydc/buster 5.6.1-330 amd64
```

3. Execute the apt install or apt-get install commands to install Delinea packages. For example: `apt-get install CentrifyCC`

   Note: To uninstall the Cloud Client rpm, you can use the remove command to delete the Cloud Client package or the purge command to also delete any configuration files. For example:

   ```
   \# apt remove centrifycc=20.6-121
   ```

To Set Up and Configure an Alpine Linux Repository

1. To configure the repository automatically, run the following commands:

   ```
   sudo apk add --no-cache bash
   curl -1sLf \ 'https://cloudrepo.centrify.com/<URLtoken>/apk/setup.alpine.sh' \ | sudo -E
   bash
   ```

   Note: Enter your Delinea repository URL token in place of **<URLtoken>**.

2. Or, if you want to manually configure the repository, run the following commands:

   ```
   curl -1sLf 'https://cloudrepo.centrify.com/<URLtoken>/apk/rsa.5DD8742729E6E4B2.key' >
   /etc/apk/keys/apk@centrify-5DD8742729E6E4B2.rsa.pub
   curl -1sLf
   'https://cloudrepo.centrify.com/<URLtoken>/apk/config.alpine.txt?distro=alpine&codename
   =v3.13' >> /etc/apk/repositories
   apk update
   ```

   When configuring the repository manually, you reference the Delinea public RSA key: `apk@centrify-5DD8742729E6E4B2.rsa.pub`.

3. Execute the apk add command to install the Delinea packages. For example: `# apk add centrifycc`

To uninstall the Cloud Client for Linux rpm, you can use the del command to delete the Cloud Client for Linux package. For example:

```
\# apk del centrifycc=5.8.0-xxx
```

Customizing Cloud Client Parameters

You can control client operations or default behavior through the following configuration parameters that you set:

- "Linux NSS-Related Parameters" below
- "Linux PAM-Related Parameters" on the next page
- "Other Configuration Parameters" on page 76

You can modify these parameters by using the cedit command. For details, see "Using Cloud Client Commands" on page 111.

Linux NSS-Related Parameters

The following are user query or NSS parameters that you can set on Linux systems:

Parameter Name	Description	Default Value
`nss.group.ignore`	Names of groups to ignore	`File:/etc/centrifycc/group.ignore`
`nss.user.ignore`	Names of users to ignore	`File:/etc/centrifycc/user.ignore`
`agent.nss.program.ignore`	Programs where CentrifyCC NSS library should not process NSS calls. Must be careful about this as cloud users will not be processed. This is renamed in 19.6 due to conflict with DirectAudit configuration parameters	kcm
`nss.group.skip.members`	List of programs that do not care about group members when getgrXXX() APIs are called	`ls,chown,find,ps,chgrp,dtaction,dtwm,pt_chmod,adid,ll,id`
`nss.programs.force.grouplist.backend`	List of process names that will get the list of all available groups from backend	none
`nss.programs.get.allmembers`	List of process names that gets group member list from backend, resulting in all members are returned. >**Note**: This will slow down system performance. DO NOT set this unless absolutely necessary.	none

Parameter Name	Description	Default Value
`nss.getgrouplist.interval`	How frequent to get the list of available groups from backend.	4 hours
`nss.prefetch.users`	List of users that the cloud client will retrieve from the Cloud service before the system requests it.	none
`nss.programs.getusergroups`	List of process names such that getpwnam/getpwuid calls by such process will also get the list of groups that the user belongs to.	nscd,su,login,sshd,sudo,groups,id,getent
`nss.refresh.prefetch.users.interval`	nss.refresh.prefetch.users.interval	1 hour
`nss.group.members.async.refresh`	whether group membership lists are refreshed asynchronously when expired information is encountered. >**Note**: DO NOT USE. Does not make sense in new group membership architecture as group membership is acquired from local cache.	`false`

Linux PAM-Related Parameters

The following are Linux user login parameters for:

Parameter Name	Description	Default Value
`pam.homedir.create`	Create home directory if it does not exist on the local machine.	`True`
`pam.homedir.create.mesg`	Message displayed when a user's home directory is created.	Created home directory

Parameter Name	Description	Default Value
pam.ignore.users	Name of users that will be authenticated locally.	file:/etc/centrifycc/user.ignore
pam.mfa.disabled	Specify whether to disable multi-factor authentication (MFA) user login on this machine.	False
pam.mfa.program.ignore	Specify a list of programs that ignore MFA.	ftpd profiled vsftpd java http cdc_chkpwd kdm unix2_chkpwd
pam.mfa.oob.max.count	Maximum number of retries for MFA for out of band mechanisms. An "out of band" mechanism is an authentication mechanism that requires additional interaction from the user, such as clicking a link in an email or SMS message.	300
pam.password.enter.mesg	Message displayed when prompting for a user's password.	Password

Other Configuration Parameters

The following are other parameters that you can configure; these apply to Windows, Linux, or both:

Parameter Name	Description	Default Value	Applicable Platforms
agent.tcp.connect.timeout	Specifies when TCP CONNECT should timeout.	30 seconds	All
agent cert.validate	Specifies whether to validate the certificate when connecting to the platform	true	All
agent.http.timeout	Generic HTTP timeout The value that you specify must be parsable into a time duration value.	2 minutes	All
agent.online.status.refresh	Determines how often the client connects to the platform to update connection status.	1 minute	All

Parameter Name	Description	Default Value	Applicable Platforms
agent.ping.timeout	Maximum time to wait for a response from the platform when updating connection status. The client will switch to offline mode after the timeout limit. The value that you specify must be parsable into a time duration value.	20 seconds	All
agent.update.interval	Determines how often the client updates the platform with its operating system and client version information.	24 hours	All
agent.web.proxy.global	The proxy URL to use when connecting to the platform. See "Additional Notes" on page 80 below.	(none)	All
agent.web.proxy.order	The web proxy order to use when connecting to the platform. See "Additional Notes" on page 80 below.	Global, Direct	All
audittrail.targets	Audit trail targets (1 - DirectAudit, 0 - not sent to DirectAudit). See "Additional Notes" on page 80 below.	1	All
cagent.audit.session	Determines if session auditing is enabled. 0 - not enabled, 1 - enabled. To change the setting, run `dacontrol -d` to disable auditing or `dacontrol -e` to enable auditing. Do not use cedit to edit this parameter.	1	Linux only
cclient.cache.cleanup.interval	How often the client cleans up the cache.	10 minutes	Linux only

Parameter Name	Description	Default Value	Applicable Platforms
cclient.cache.expires	Amount of time until a generic object is checked in to the platform for changes.	1 hour	Linux only
cclient.cache.member.refresh	Amount of time that must pass before a group membership object is expired.	30 seconds	Linux only
cclient.cache.negative.expires	Lifetime of a negative object in cache.	5 seconds	Linux only
cclient.cache.password.hash	Specifies whether to store the password hash for client-based login.	True	Linux only
cclient.cache.refresh	Amount of time that must pass before an object is refreshed from the platform.	5 minutes	Linux only
cenroll.agent.wait.time	Determines how long the cenroll command should wait for the client to create its LRPC socket and serve requests before it runs the post-enroll script and exits. The value that you specify must be parsable into a time duration value.	10 seconds	All
cenroll.http.timeout	HTTP timeout for enroll and unenroll commands. The value that you specify must be parsable into a time duration value.	5 minutes	All
cli.hook.cenroll	The path to the post-enrollment script, if you've configured one.	none	All

Parameter Name	Description	Default Value	Applicable Platforms
`CloudUserDomains` (Windows only)	This value is a comma-separated list of domains. During initauth if the username is in UPN format and the domain part matches the one from the `CloudUserDomains` list, it will be treated as a cloud user and the username will not try to be resolved in Active Directory. This setting replaces the boolean `CloudFirstUserLookup`.	false	All
`EnableCSSExtension`	Used to enable or disable the CSS Extension. Enabling this feature allows zone role workflow requests to process immediately and not be delayed by Active Directory synchronization schedules.	false	Linux
FeatureAAPMEnabled	Used to enable or disable the AAPM feature.	none	All
`FeatureAgentAuthEnabled`	Used to enable or disable the Agent Auth feature.	none	All
`FeatureDMCEnabled`	Used to enable or disable the delegated machine credentials feature.	none	All
`LogLevel`	Log level (used for client log only). The best practice is to create a varying parameter or LogLevel that shows the log level for all items, with the exception of Linux user query or Linux user login.	Info	All

Parameter Name	Description	Default Value	Applicable Platforms
log.rest	If this is set to true, the client will log REST API calls and return values as INFO level messages. If this is set to false, the client logs these operations as DEBUG level messages.	false	All
log.script	Perl script logging level.	Info	Linux only
log.script.autoedit.pl	Perl script logging level for autoedit.	Info	Linux only
lrpc2.client.connect.timeout	LRPC2 client (other than Cloud Client) connection timeout	5 seconds	All
lrpc2.client.receive.timeout	Amount of time that lrpc2 client will wait for reply from the Cloud Client	5 minutes	All
lrpc2.client.send.timeout	Amount of time that lrpc2 will wait for the Cloud Client to receive the LRPC2 client request	1 minute	All
print_log_to_stdout.script	Perl script logging redirect to stdout	1	Linux only
recurring.interval.deviation.percentage	The maximum percentage deviation allowed for adding randomness to the interval between runs in a recurring job.	5	All

Additional Notes

For proxy settings, review the following in the Cloud Client:

- If the setting proxy is empty, all REST API calls are sent directly to the platform.
- If the setting proxy is non-empty, it is used as the proxy for all REST API (including enrollment).
- The user can specify which proxy to use in the cenroll command. The parameter impacts the proxy setting.
- The upgrade process handles agent.web.proxy.order and agent.web.proxy.global as follows:

  - If the first value of agent.web.proxy.order is direct, set proxy setting to empty. This applies only to direct connection.
  - Otherwise, import the value of agent.web.proxy to proxy parameter in settings package.
- If direct connection fails, there is no proxy support.

Enabling Client Features

You can enable or disable the Cloud Client features for enrolled Windows or Linux systems either from the command line or from the Client Profile in the Admin Portal.

For example, you can enable features such as delegated machine credentials, AAPM, or client-based login (AgentAuth).

Note: Feature management is available on systems with Cloud Client version 20.7 or later.

To enable or disable client features in the Admin Portal:

1. In the Admin Portal, go to **Systems**, and select the computer for which you want to enable or disable features.
2. In the system page, click **Client Profile**.
3. In the **Client Features** section, click the checkbox next to any feature that you want to enable; deselect any checkboxes next to features that you want to disable.
4. Click **Save**.

To enable client features at the command line:

1. Log in to the system for which you want to enable or disable features.
2. In a command line or terminal window, run the cedit command to set the feature parameters. For example, if you want to enable delegated machine credentials, you'd enter the following:

   ```
   cedit -s 'FeatureDMCEnabled:true'
   ```

For a list of parameters that you can use with [cedit], see "Customizing Cloud Client Parameters" on page 73.

Enabling the CSS Extension

Enabling the CSS Extension

You can enable the CSS Extension on the Cloud Client for Linux so that when you do a zone role workflow request, you don't have to wait for Active Directory to synchronize by way of the Cloud Connector. When the CSS Extension is enabled, after a zone role workflow request is approved the requester can access the specified system(s) immediately.

You can enable the CSS Extension by doing either of the following:

- During enrollment, specify -css or -C to enable the CSS Extension with the cenroll command.

  ```
  cenroll --css
  ```

(plus the other parameters to complete the enrollment)

- After enrollment, use the cedit command with the EnableCSSExtension parameter to enable the CSS Extension.

  ```
  cedit -s EnableCSSExtension:true
  ```

If you set up zone role workflow with just the Cloud Connector, be aware that there will be a delay between when the approver approves the request and when the user can access the affected systems. Although the Cloud Connector updates Active Directory immediately after the approver approves the request, a delay occurs because it can take some time to replicate the Active Directory information and also because the Server Suite Agent reloads authorization information from Active Directory at specified intervals.

Note: The client channel and the CSS Extension aren't supported for Hyper-scalable PAS deployments.

Enabling Client-Based Login

Client-based login is a way that you can use the Cloud Client to log in to other systems that you have registered in Privileged Access Service. There are two main components to enabling client-based login:

- Grant client-based login permission (also called the AgentAuth permission) to the desired user accounts or roles.
- Enable the client-based login feature (also called the AgentAuth feature) when you enroll a system with the Cloud Client.

Below is some information about how client-based login differs on Windows and Linux systems, and then how to enable client-based login.

About Client-based Login on Windows

The first time that you log in to a Windows system using client-based login, the service creates a new, local user that corresponds to your Privileged Access Service account if your account is a Delinea Directory or a federated account. Each time that you log in this way the service rotates the password to a random string of 32 characters. If your account is based in Active Directory, the service does not create a local account for you; you log in with your Active Directory credentials.

The service also assigns this user to local groups according to local group mapping rules that you have configured. Any changes that you make to the local group mapping configurations take effect the next time the user logs in. If an affected user is currently logged in when you make the changes, the changes take effect after the user logs out and logs in again.

This local user operates as a background user and does not show up in any lists of local users inside of Privileged Access Service; you can see this local user in the Local Users and Groups on Windows. This local account stays provisioned until you uninstall the client.

Removing the Windows Local Account

You can choose to remove this local Windows user account when the session terminates; the setting is Removing local accounts upon session termination - Windows only. Removing the local account helps fulfill compliance requirements and also helps facilitate just-in-time (JIT) privilege elevation with ephemeral account provisioning, in conjunction with local group mapping and the client-based login (Agent Auth) workflow.

In general, administrators configure client-based login with local group mapping as follows:

- Enable the Agent Auth Workflow in a policy that applies to all systems, a set, or the individual system
- Map the user's role to the Administrators group
- Enable the setting to remove local account in a policy that applies to the desired scope

Here's an example of how the process of just-in-time privilege elevation works; this example involves a user named Kayla who needs to run some administrator scripts on a Windows system:

The administrators have already enabled the Agent Auth feature on the Windows system. They have specified that the service will delete the local Windows account upon session termination; they have specified this using a policy.

For more information, see the following topics:

- "Installing and Using the Cloud Client for Windows" on page 41.
- "Enabling the AgentAuth feature and Granting the AgentAuth Permission" below
- Using Agent Auth workflow

1. Kayla requests and receives permission to log in to the designated Windows system:
   a. She logs in to the Admin Portal and navigates to the desired Windows system.
   b. She follows the Agent Auth workflow to request permission to access a particular Windows system.
   c. Her manager approves the request and grants Kayla permission for 1 hour.
2. Kayla logs in to the designated Windows system successfully.

   Upon login, the service creates a local admin account and provisions it into the Administrators group based on the local group mapping (configured by the administrator).
3. She performs the necessary work on the Windows system.
4. Kayla logs out of the designated Windows system.

   The service deletes the local Windows account that was created in Step 3 and revokes all access for that account. The user will need to request login permissions when needed.

About Client-Based Login on Linux

The first time that you log in to a Linux system using client-based login, the PAM and NSS modules for the Cloud Client handle the authentication and group membership of your account. The service does not create a local user account. If desired, you can modify any default Linux user configuration settings under **Settings** > **Enrollment** > **Linux Settings**.

Enabling the AgentAuth feature and Granting the AgentAuth Permission

To enable client-based login for a system and a user or role

1. Enroll the computer in the Privileged Access Service and enable the AgentAuth feature.

   In the Cloud Client for Windows installer, you can enable all features by not entering anything in the Optional Parameters section. Or, you can enter AgentAuth as a parameter to only enable client-based login.

If you're using the cenroll command either on Windows or Linux, you can include either of the following options to enable either just the client-based login or all features:

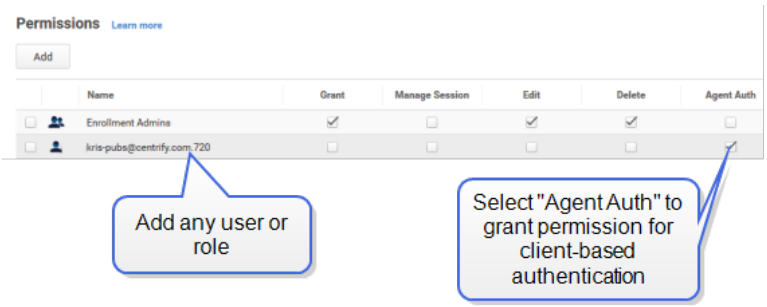
```
\--features AgentAuth
\--features All
```

You can also enable Cloud Client features in the Admin Portal. For details, see "Enabling Client Features" on page 81.

For details about Cloud Client commands and options, see "Using Cloud Client Commands" on page 111.

2. Log on to the Privileged Access Service.
3. Click **Resources > Systems**, then click the computer you registered to display its details.
4. Click **Permissions**.
5. Click **Add**, if necessary, to find and select the user account or role, then select **Agent Auth**.

   For example, if you want to add client-based login for the user kris-pubs@acme.com.720 on this computer, you would add the user to the list of accounts that have permission on the system then select the Agent Auth permission.



Note: You can configure client-based login for a specific system or a set of systems.

6. Click **Save**.

Adding a Role for Client-Based Login

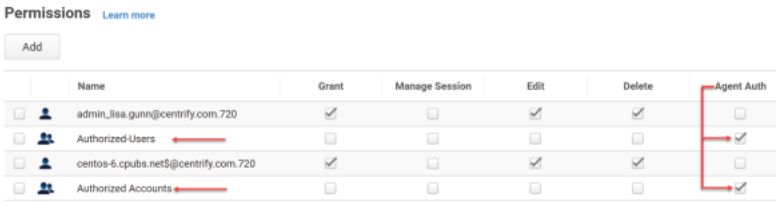
To simplify the process of authorizing users, however, you can add one or more roles specifically for client-based login. You can then specify the appropriate roles during registration to immediately grant role members access to the system.

Preparing a role for authentication is particularly useful If you are automating the deployment of virtual machine instances using a script. By specifying one or more roles in the script using the `--agentauth` option, you can ensure users can log on immediately after the system is successfully registered.

For example, an automation script might include a command similar to the following to register a computer in the Privileged Access Service and enable members of the **Authorized Accounts** role to log on:

```
sudo cenroll --tenant abc1234.my.centrify.net--code A1BC2345-D6E7-89F0-G123-HIJK4LM5N67P --
features all --agentauth “Authorized Accounts”
```

For example, if the computer you registered was centos-6.cpubs.net and you specified **Authorized-Users** and **Authorized Accounts** as the roles than can have members authenticated, the system would automatically add these roles to the system with the **Agent Auth** permission set.



The role you use for client-based login does not require any special administrative rights.

Logging on for the First Time

Users who are authorized to log on to computers where the Cloud Client for Linux is installed with the client-based authentication, must use their full account name the first time they log on. For example, Active Directory users should log on using **user-name@domain** format. Privileged Access Service users should log on with a valid suffix for their Privileged Access Service instance. For example, if the suffix you use for the Privileged Access Service instance is acme.com, the first time you log on you would use **user-name**@acme.com.

Authenticating with a Single-Use SSH Certificate

In some environments, it is useful to be able to log on to selected computers using authentication that doesn't require a password. The **Use My Account** feature allows you to enable secure shell sessions that do not require a password for the following Server Suite-managed computers:

- Computers joined to an Active Directory domain using the Server Suite Agent for *NIX or Server Suite Agent for Windows.
- Computers registered in the Privileged Access Service using the Cloud Client for Linux or Cloud Client for Windows.

For example, if you use a smart card to authenticate your identity, authentication relies on a public and private key exchange using encrypted certificates instead of a password or personal identification number.

Note: This feature is now supported for PAS web-based SSH client sessions and if you are accessing a target system using native SSH clients.

The following is an overview of the steps required to enable **Use My Account** using the PAS browser-based secure shell client (detailed instructions are provided in subsequent sections):

1. Verify the computers you want to access remotely meet basic system requirements. For details, see "Prerequisites for Use My Account" on the next page.
2. Determine which SSH daemon version is running on the target system. For details, see "Confirming the SSHD version" on the next page.
3. Download the SSH master key file, which is a public file that must be installed on each target system you want to access. For details, see "Downloading the SSH Master Key File" on the next page.

4. Update the system settings in the Admin Portal to identify the computers you have configured to use the SSH master key and existing accounts. For details, see "Updating System Settings to Allow Use My Account" on page 88.
5. Modify the sshd_config file on each target system. For details, see "Modifying the SSHD configuration file for the Cloud Client" on page 89.

Prerequisites for Use My Account

To use the **Use My Account** feature, your environment must meet the following minimum requirements:

- Privileged Access Service 18.3 or later
- Delinea-compiled or standard/native OpenSSH version 7.4 or later
- The Cloud Client for Linux version 18.3 or later
- Brokered authentication components from release 2018 or later

> **Note:** You cannot use the feature to log on with a federated user account.

Confirming the SSHD version

Perform the following procedures to determine which of the following SSHD versions your system is using:

- Standard OpenSSH (used with Cloud Client and Server Suite Agent configurations)
- Delinea-compiled OpenSSH (used with Server Suite Agent configurations only)

To confirm the SSHD version you are using:

1. Access the target UNIX system where you intend to download the SSH master key file.
2. Run the following command to determine which SSH daemon is running (the standard OpenSSH or Delinea-compiled version):

   >ps -ef | grep sshd
3. Note which SSH daemon is running:

   If the result is: /usr/sbin/sshd, you are running the standard OpenSSH version.

   If the result is: /usr/share/centrifydc/sbin/sshd, you are running the Delinea-compiled version.
4. Next you need to download the SSH master key file. For details, see "Downloading the SSH Master Key File" below.

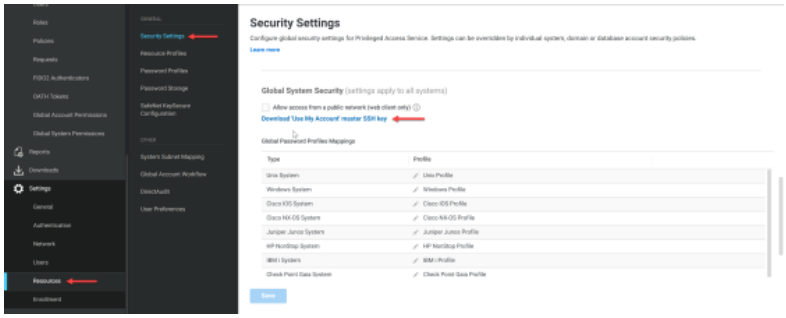
Downloading the SSH Master Key File

Download the SSH master key file onto each target system you want to access. The SSH master key file is a public file that you can download using the Admin Portal or a UNIX command line.

To download the SSH master key file from the Admin Portal:

The following must be performed on the target system.

1. In the Admin Portal, click **Settings**, then click Resources to display the settings available for Privileged Access Service.
2. Click **Security Settings**.
3. Click **Download 'Use My Account' master SSH key**.



4. Click the link to download the file, then click **OK**.
5. Rename the **ca.pub** file you just downloaded to:

   centrify_tenant_ca.pub.
6. Save the SSH master key file you just downloaded to one of the following locations depending on your SSHD version:
   - For the standard OpenSSH version, save the SSH master key file to: /etc/ssh/centrify_tenant_ca.pub
   - For the Delinea-compiled OpenSSH version, save the SSH master key file to: /etc/centrifydc/ssh/centrify_tenant_ca.pub
7. Now that you have downloaded the SSH master key file and saved it, you need to update the system settings to allow **Use My Account**, see "Updating System Settings to Allow Use My Account" on the next page

To download the SSH master key file from a UNIX command line

1. Execute a wget or curl command to download the SSH master key file from a UNIX command line.
   - If you are running the standard OpenSSH package enter:

     ```
     curl -o /etc/ssh/centrify_tenant_ca.pub https://\<customer tenant URL\>/servermanage/getmastersshkey
     ```

     For example, if the customer-specific tenant URL is abc1234.my.centrify.net:

     ```
     curl -o /etc/ssh/centrify_tenant_ca.pub https://abc1234.my.centrify.net/servermanage/getmastersshkey
     ```
   - If you are running the Delinea-complied OpenSSH package enter:

     ```
     curl -o /etc/centrify/ssh/centrify_tenant_ca.pub https://\<customer tenant URL\>/servermanage/getmastersshkey
     ```

     For example, if the customer-specific tenant URL is abc1234.my.centrify.net:

     ```
     curl -o /etc/centrify/ssh/centrify_tenant_ca.pub https://abc1234.my.centrify.net/servermanage/getmastersshkey
     ```

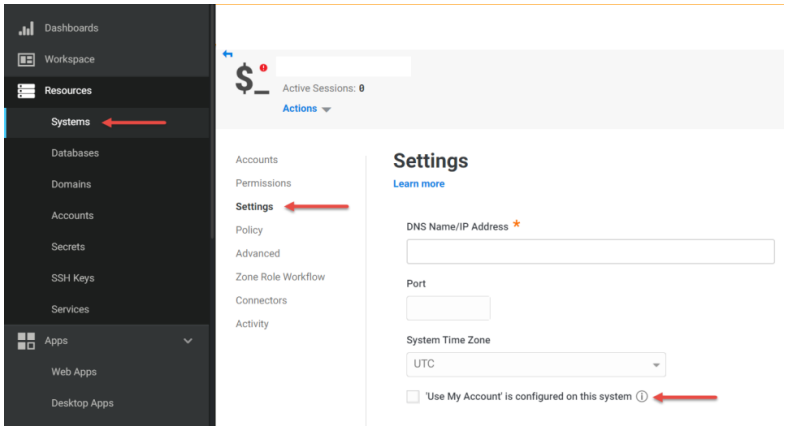
2. Save the SSH master key file you just downloaded to one of the following locations depending on your SSHD version:
   - For the standard OpenSSH version, save the SSH master key file to: /etc/ssh/centrify_tenant_ca.pub
   - For the Delinea-compiled OpenSSH version, save the SSH master key file to: /etc/centrifydc/ssh/centrify_tenant_ca.pub
3. Now that you have downloaded the SSH master key file, you need to update the system settings to allow **Use My Account**, see "Updating System Settings to Allow Use My Account" below

Updating System Settings to Allow Use My Account

After downloading the SSH master key file, you can modify the system settings to allow any user with view permissions and an account on that system to log on.

To enable Use My Account

1. In the Admin Portal, click **Resources**, then click **Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Select **Settings** and then select **Use My Account** to enable secure shell sessions without a password.



Once the **Use My Account** option is enabled for a system, the action is visible to all users even if they don't have an account available. If users without an account select the action, however, the logon attempt will fail with an error message.

> **Note:** When logging in as an Active Directory user on an Active Directory-joined machine, you will see a dialog box asking to enter a username.

4. Next you need to modify the SSHD configuration file (see one of the instructions below). Select the instruction applicable to your configuration.
   - For computers joined to an Active Directory domain using the Server Suite Agent, see "Modifying the SSHD Configuration File for the Server Suite Agent" on the next page.
   - For computers registered using the Cloud Client, see "Modifying the SSHD configuration file for the Cloud Client" on the next page.

Modifying the SSHD configuration file for the Cloud Client

If a computer is registered in the Privileged Access Service using the Cloud Client, do the following:

1. Locate the sshd_config file, located here:
   ```
   vi /etc/ssh/sshd_config
   ```
2. Locate or add these values to the file:
   ```
   TrustedUserCAKeys /etc/ssh/centrify_tenant_ca.pub
   ChallengeResponseAuthentication yes
   UsePAM yes
   ```
   Note: On some more recent OS's the ChallengeResponseAuthentication parameter may have been replaced with KbdInteractiveAuthentication parameter.
3. Restart the sshd program after updating the configuration for the changes to take effect.

   For example, as root you might run one of the following commands to restart the daemon:
   - `systemctl restart centrify-sshd`
   - `service centrify-sshd restart`

     If you are using the OpenSSH version of SSHD, the following commands can be used to restart the daemon:
   - `Service sshd restart`
   - `Sudo systemctl restart sshd`

Modifying the SSHD Configuration File for the Server Suite Agent

If a computer is joined to an Active Directory domain using the Server Suite Agent, add lines similar to the ones indicated in this procedure to specify the name and location of the downloaded SSH master key file in the sshd_config file.

1. Locate the sshd_config file based on the following:
   - If you are using standard OpenSSH, use the following file: `/etc/ssh/sshd_config`
   - If you are using Delinea-compiled OpenSSH, use the following file: /etc/centrifydc/ssh/sshd_config
2. Determine the computer type and then set the AuthorizedPrincipalsCommand property in the sshd_config file to one of the following:

Computer Type	SSHD Config File Line

Standard	`TrustedUserCAKeys /etc/ssh/centrify_tenant_ca.pub`
	`AuthorizedPrincipalsCommandUser root`
	`AuthorizedPrincipalsCommand /usr/bin/adquery user -P %u`

CoreOS	`AuthorizedPrincipalsCommand /usr/bin/adquery user -P %u`

3. Restart the sshd program after updating the configuration for the changes to take effect.

   For example, as root you might run one of the following commands to restart the daemon:

- `systemctl restart centrify-sshd`
- `service centrify-sshd restart`

Logging on with an expired password

If you want to allow users to log on to Delinea-managed computers even if their password has expired in Active Directory, there are additional configuration steps you must perform.

- On each Delinea-managed computer where you want to support the **Use My Account** feature, open the centrifydc.conf file (etc/centrifydc/centrifydc.conf) and verify the following parameter is set to true or not set (the default is true):

  `pam.allow.password.expired.access: true`

- Then edit the appropriate files as shown below:

System Type	Edit File	

Red Hat Linux computers (system-auth)	- Access the /etc/pam.d/system-auth file.
	- In the auth line add deny_pwexp.
	- In the account line add skip_pwexp_check.
	For example:
	`auth sufficient pam_centrifydc.so deny_pwexp ...`
	`account sufficient pam_centrifydc.so skip_pwexp_check`	

SuSE Linux computers (common-auth and common-account)	- Access the /etc/pam.d/common-auth file. - Edit the auth line. - Access the `/etc/pam.d/common-account` file.	- Edit the account line.

Solaris, HPUX, and AIX with standard SSHD (pam.conf)	- Access the /etc/pam.conf file.
	- Edit the auth and account lines for ssh service.
	For example:
	`ssh auth sufficient pam_centrifydc deny_pwexp`
	`...`
	`ssh account sufficient pam_centrifydc skip_pwexp_check`	

Note: Changes to the auth and account settings affect all login-related services.

Working with Privilege Elevation

Privilege elevation provides a way for users to log in as themselves with limited privilege and then request to elevate their access in order to perform privileged operations. Users can then provide additional MFA credentials to continue and run the privileged commands or applications.

By using privilege elevation, you grant access based on Zero Trust principles and then grant privileged access only when needed for a specific operation.

How Privilege Elevation Works

Privilege elevation works on both Windows and Linux systems, with some slight differences.

An Example of How Privilege Elevation Works on Windows Systems

Note: Offline Privilege Elevation isn't supported on Windows.

1. The admin configures the Windows system so that the `bob@acme.com` account has privilege elevation access and sets a policy that anyone logging in Monday through Friday needs to provide a password when running privileged applications or commands.
2. User `bob@acme.com` logs on to a Windows system on a Tuesday with just enough privilege to do normal tasks.
3. Bob needs to run some PowerShell scripts as Administrator. He opens a PowerShell Administrator window.

   An elevation consent dialog box displays.
4. Bob selects **Run with Privilege**.
5. Because of the privilege elevation policy, the service prompts him for his password.

   After the user enters the correct, additional authentication credentials, he can run the privileged application.

An Example of How Privilege Elevation Works on Linux Systems

Note: For offline Privilege Elevation to work on Linux, set the option in **/etc/sudoers** to `timestamp_timeout=0`. This impacts default behavior where a user will always have to reauthorize, but it allows our offline login to work.

1. The admin configures the Linux system so that the `bob@acme.com` account has privilege elevation access and sets a policy that anyone logging in Monday through Friday needs to provide a password when running privileged applications or commands.
2. User `bob@acme.com` logs on to a Linux system on a Tuesday with just enough privilege to do normal tasks.
3. Bob needs to run `cdiag` as root, so at the terminal, he enters the following command:

   ```
   sudo cdiag
   ```
4. Because of the privilege elevation policy, the service prompts Bob to enter his password.

   After the user enters the correct, additional authentication credentials, he can run the privileged command.

Using Sudo Plugin to Run Commands as Another User

The sudo plugin runs a command as another cloud or local user on the linux system.

Note: This feature is for Linux only.

1. In the **Admin Portal**, go to **Settings**> **Resources** > **Privilege Elevation Command**.
2. You can add a new command or select a current command to edit or change it.
3. Once you are in a new command or modifying an existing command, click the **Run as User** box.
4. Add the username you'll use to run as a local user or a cloud user:

- To run as a local user input **yourusername@localhost**.
- To run as a cloud user, specify the UPN name and **user@suffix**.

After following the above steps your request to run a command as a different user goes to the cloud service. The following outcomes can happen:

- If the command is allowed, the command runs on the system.
- If the command is not allowed but workflow is enabled, then you can send a workflow request.
- If the command is not allowed to run and workflow is not enabled, then a message will appear saying that you are not allowed to run that command as the runas user.

You can now, as User A, run a command as User B according to the policy rules.

Privilege Elevation Requirements

In order to have your users be able to use privilege elevation on a system, here are the requirements:

- **Administrative rights:** You the administrator need to have these permissions:
  - Privilege Elevation Management administrative rights – (assigned to your role) in order to grant privilege elevation access to others. For details, see Admin Portal administrative rights
  - Add Privilege Elevation permission – this can be set either on a specific system, a set of systems, or globally.
- **Enrollment:** Install and enroll the Cloud Client on the desired systems. For details, see "Installing and Using the Cloud Client for Windows" on page 41 and "Enrolling and Managing Computers Using the Cloud Client for Linux" on page 53.
- **System permissions:** Enable the Agent Auth (client-based login) feature for the affected systems. For details, see Setting system-specific permissions.
  - The Server Suite Agent cannot be installed on the same computer; if the Server Suite Agent is also installed, you can't enable Agent Auth.
- **Privilege elevation access:** Configure privilege elevation access to users, roles, or groups for a specific system, a set of systems, or all systems (see the procedures below)
- **Force MFA policies:** If desired, configure privilege elevation authentication policy settings to enforce MFA at elevation–when users go to run an privileged application or command on a designated system. You can set the policy for a single system, a set, or for all systems. For details, see Setting system-specific policies.
- **Commands and applications with elevated privilege:** To control access to commands or applications with elevated privilege, define the commands in the global Settings > Resources > Privilege Elevation Command page. For details, see "Specifying Privilege Elevation Commands and Applications" on page 95.

Note: If you try to elevate privileges for a user whose account name has 16 or more characters in it, privilege elevation fails with an error.

Configuring Privilege Elevation Access

There are a few tasks you perform when configuring privilege elevation access:

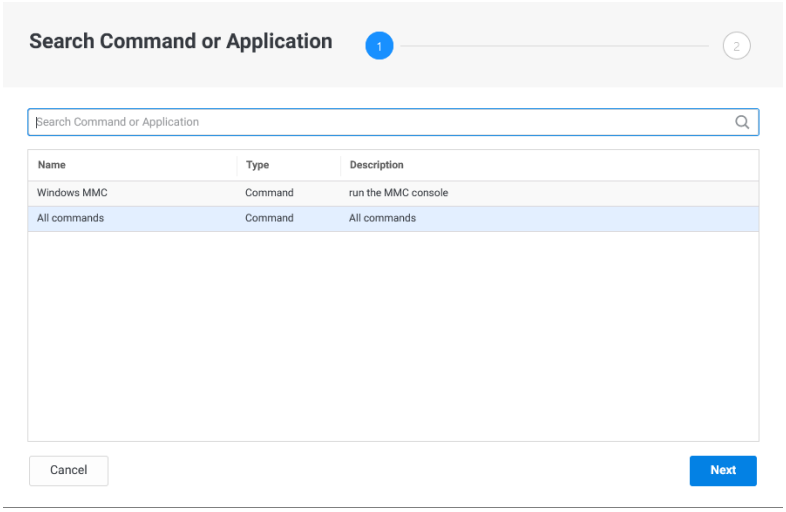
1. "Specifying Privilege Elevation Commands and Applications" on page 95. You can control access to either all commands and applications on systems or limit it to just one or more commands or applications. You specify different sets of commands or applications for Windows and Linux systems.
2. "Granting Privilege Elevation Access to Users" below (below) so that people can request applications or commands with elevated privilege on the specified systems.
3. "Configuring Privilege Elevation Challenge Rules" on the next page (below) that specify how people will get access to applications or commands with elevated privilege. The rules specify what conditions need to be met and the authentication profiles say how to authenticate the users under those conditions.

Granting Privilege Elevation Access to Users

To grant privilege elevation access to users, groups, or roles

1. Navigate to the Privilege Elevation tab for the systems that you want to grant people access to:
   - All systems (global): go to **Settings** > **Resources** > **Security** > **Global Privilege Elevation**.
   - A set of systems: In the Systems view, select the desired set and click the menu item (...) and choose **Modify**, and then click **Member Privilege Elevation**.
   - One system: In the Systems view, open the desired system, and then click **Privilege Elevation**.
2. Click **Add**.

   The Search Command or Application screen displays and includes the commands that apply to the affected system(s). For example, if you selected only Windows systems, then only Windows command options display.



3. Select the commands you want to grant access to.

   Note: If you select **All Commands** the user will be able to perform any commands on the target system with elevated privileges.

```
Click __Next__ to continue.
```

4. Search for or select the users, groups, or roles that you want to grant access to, select them in the results list, and click **Add**.

   The users, groups, or roles that you added now display in the list on the Privilege Elevation tab. Users, groups, or roles added here must have the Agent Auth permission on the affected system.

   If you specify permissions at the set or global level, you can see the inherited permissions when you view a single system affected by those settings.

   Note: The ability to configure a valid date or time span when the privilege elevation applies is coming in a later release. For now, ignore the Starts and Expires columns.

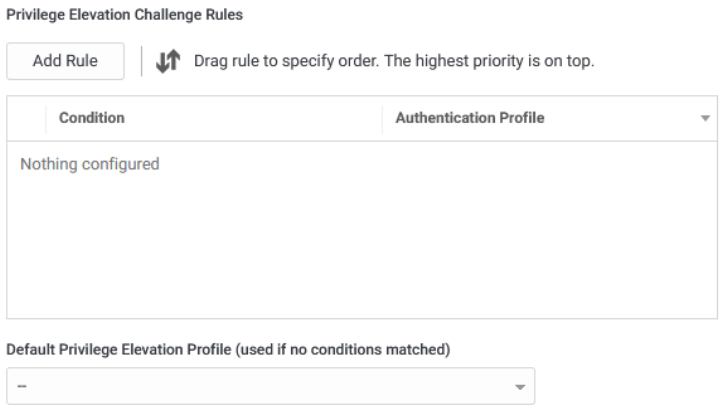
5. If desired, you can select **Bypass MFA** for any of the users, groups, or roles that you've granted privilege elevation access to. Selecting this option grants them access but they don't have to provide any additional authentication credentials.
6. Click **Save** to save your changes.

   Your designated users can now run applications with elevated privilege on the designated systems.

Configuring Privilege Elevation Challenge Rules

To configure privilege elevation challenge rules and default authentication profiles

1. Open the policy tab for the desired systems:
   - One system: In the **Systems** area, open the desired system, then click the **Policy** tab.
   - Some or all systems: In the **Policies** area, open or edit a policy set.
2. In the policy, navigate to **Resources** > **Systems**, and then the **Privilege Elevation Challenge Rules** section of the page.



3. In the **Privilege Elevation Challenge Rules** area, add rules that specify for a particular condition, apply a particular authentication profile.
4. For the **Default Privilege Elevation Profile**, specify which authentication profile applies if none of the conditions in the challenge rules are met.
5. Click **Save** to save your changes.

The challenge rules and default authentication profile changes for privilege elevation take effect when the affected users next log try to run an application with privilege on an affected system.

Specifying Privilege Elevation Commands and Applications

You can control access to specific commands and applications on Windows and Linux systems, and you can even specify which arguments a user can pass to a privileged command. You specify which commands and applications to restrict access to as part of your overall privilege elevation security controls.

Examples of Windows Elevated Privilege Commands and Apps

Here are some examples of Windows elevated privilege commands and applications, which you could include in a command set entitled "Windows Management Tools" or something similar:

Privilege elevation command name	Application and Arguments	Path
Server Manager	ServerManager.exe	Standard system path
Service Control Manager	sc.exe	Standard system path
Microsoft Management Console (MMC)	mmc.exe	Standard system path

Examples of Linux Elevated Privilege Commands and Apps

Here are some examples of Linux elevated privilege commands and applications, which you could include in a command set entitled "Linux commands" or something similar:

Privilege Elevation Command Name	Command	Glob or Regular Expressions	Match Path	Description
Edit SSH server config	`vi /etc/ssh/sshd_config`	Glob expression	Standard user path	Allows the granted user to edit the SSH server's config file but nothing else.
Edit SSH	`vi /etc/ssh/\*_config`	Glob expression	Standard user path	Allows the granted user to edit any SSH-related configuration.

Privilege Elevation Command Name	Command	Glob or Regular Expressions	Match Path	Description
Change firewall	`iptables -A INPUT -s \* -j ACCEPT`	Glob expression	Standard system path	Allows the granted user to change Linux firewall rules so specified hosts can make network connections
Restart PostgreSQL	`systemctl restart pgsql`	Glob expression	Standard system path	Allows the granted user to restart the PostgreSQL service
Linux Start/Restart Service	`^(systemctl) (restart|start|status) [a-zA-Z0-9_.-]*$`	Regular expression	Standard user path	Start/Restart the Linux services.
Linux Apache config file vi (m)	`^(vim?|nano) (\/etc\/httpd\/conf\/httpd.conf)$`	Regular expression	Standard user path	vi or vim Edit the Apache httpd.conf file.
Linux CClient cache flush	`^(cflush).*`	Regular expression	Standard system path	The Delinea client cache flush.
Linux Reboot Machine	`(reboot)(?!.*?halt).*`	Regular expression	Standard system path	Reboot the Linux machine with options other than --halt.
Linux Show local security log	`^(cflush).*`	Regular expression	Standard user path	Show information from the local /var/log/secure to show command attribution to the individual user.

Privilege Elevation Command Name	Command	Glob or Regular Expressions	Match Path	Description
Linux Display sudoers	`(cat|more) \/etc\/sudoer`	Regular expression	Standard user path	Display the contents of the sudoers file.
Linux cat the shadow file	`(cat|more) /etc/shadow`	Regular expression	Standard user path	View the restricted /etc/shadow file.

When you add or modify privilege elevation commands, you can also specify which user accounts the commands will run as. The **Root user** is the default. You can add one or more users by adding it under **Run Command As**.

About Linux Match Paths

When you specify a match path, you can select one of the following options:

- Standard system path
- Standard user path
- System search path
- Specify path

Here's how the match path maps to the binary directories on Linux systems:

Path Setting	Included Directories
System Path	`/sbin`, `/usr/sbin`
User Path	`/bin`, `/usr/bin`
Search Path	`/sbin`, `/usr/sbin`, `/bin`, `/usr/bin`

Here's a brief overview of how Linux uses each directory:

```
/bin : For binaries usable before the /usr partition is mounted. This /bin directory is
used for trivial binaries used in the very early boot stage or ones that you need to have
available in booting single-user mode. Think of binaries like cat, ls, and so forth.

/sbin : Same, but for binaries with superuser (root) privileges required.

/usr/bin: Same as first, but for general system-wide binaries.

/usr/sbin: Same as above, but for binaries with superuser (root) privileges required.
```

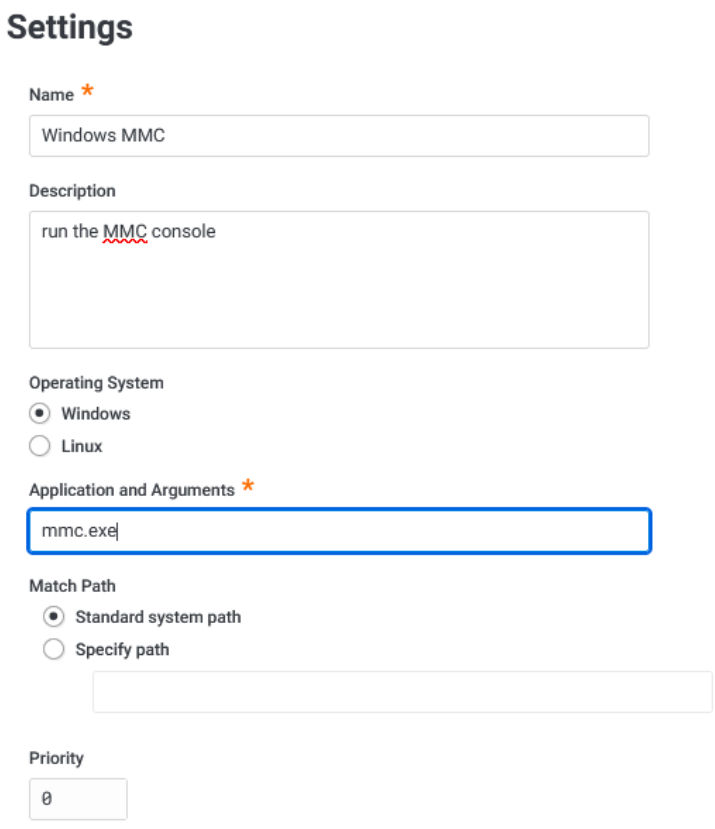
For more details about glob and regular expressions, see "About Glob Expressions" on page 101 and "About Regular Expressions" on page 101.

To Specify the Privilege Elevation Commands

1. Navigate to **Settings > Resources > Privilege Elevation Command**.
2. Click **Add**.

   The Add Command Settings page opens.
3. Enter a name and description.
4. Select the operating system: **Windows** or **Linux**.
5. If you selected **Windows**:
   a. In the **Application and Arguments** field, enter the applications or command arguments that you want to control access to.
   b. For **Match Path**, specify whether to use the default path to the command or you can select **Specify path** and enter the path manually.

      Here's an example of how to specify the MMC console:



6. If you selected **Linux**:

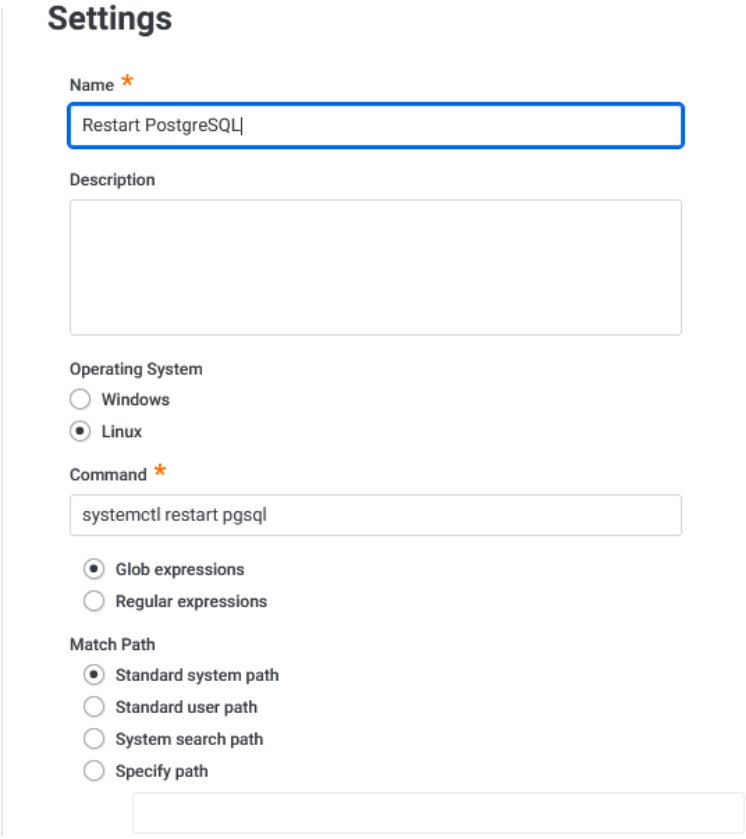
a. In the **Command** field, enter the applications or command arguments that you want to control access to.

b. If you're using regular expressions, select that option. Otherwise, keep **Glob expressions** selected.

> **Note:** If you plan to use regular expressions, note that regex support has been introduced in sudo 1.9.10, per https://www.sudo.ws/posts/2022/03/sudo-1.9.10-using-regular-expressions-in-the-sudoers-file/ . Make sure that the systems you plan to run these commands on are running at least that version of sudo.

The default glob pattern matching enables you to specify a string using wild card characters. For example, with glob pattern matching, the command can contain a question mark (?) to represent any single character, an asterisk (*) to represent any string, including an empty string, or an expression enclosed by brackets ([. . .]).

Here's an example of how to specify the command to restart PostgreSQL



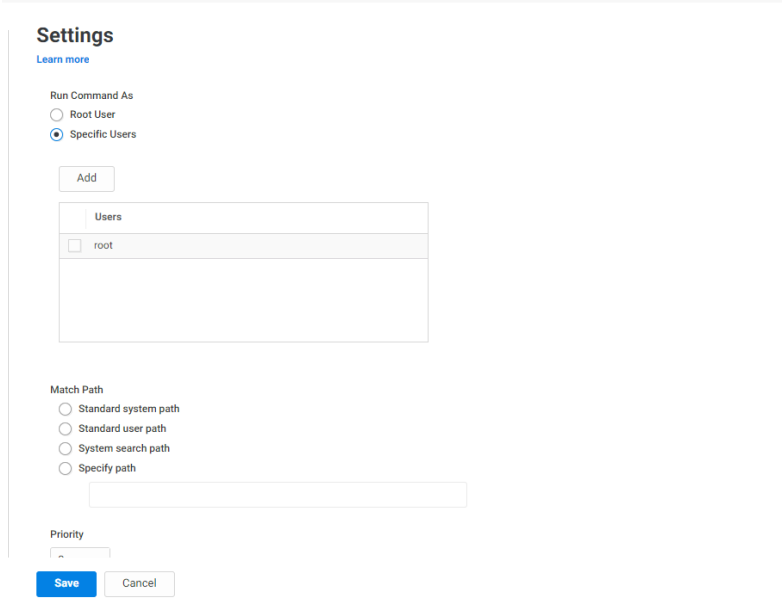
c. Select **Run Command As** and select **Root User**.

i. Or, you can configure a specific user so that the command is run as that user.

ii. Under **Specific Users**, select **Add**, enter the name of your user group.

iii. Select that group and continue.

7. In the **Match Path** select the best path where the command can be found.



8. Specify the priority.

   By default, the priority is set to 0 (zero), which indicates the lowest priority. You can specify any positive integer for this field. For example, you might want to set different privilege commands with different priorities if they have different runtime attributes (such as Bypass MFA enabled). At runtime, the privilege elevation command with the highest priority in the same operating system group is used.

9. Click **Save**.

   The service saves the command (or range of commands) and the new specification displays in the list on the Privilege Elevation Command page. You can now grant access to these commands as discussed in "Granting Privilege Elevation Access to Users" on page 93.

Add a Set of Commands

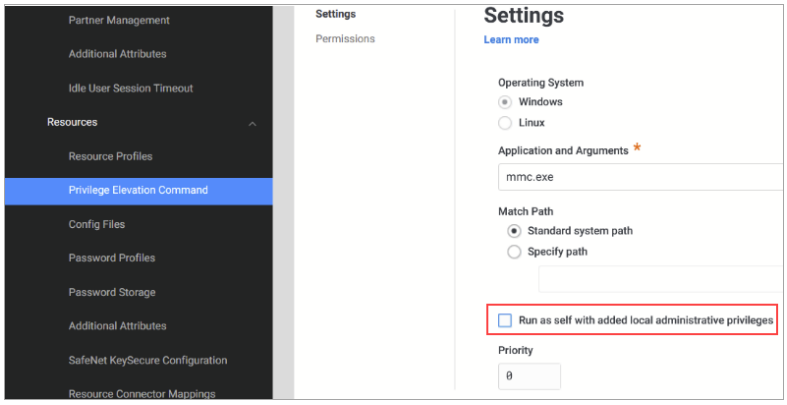
1. Go to **Settings** > **Resources** > **Privilege Elevation Command** Click **Add** listed in the **Sets** pane in the upper right.
2. Fill out **Create Set** under **Settings** list your **Name** set **Description** and select a set **Type**.
3. Click **Save**.

Privilege Elevation with Added Group Privileges for Windows

The **Run as self with added administrative privileges** option was added for users to be able to run specific commands on Windows with added group membership.

- The option is unchecked by default.
- When the option is checked, the command will run with the user that is logged into the system but with added local Administrator privileges.
- When the option is unchecked, windows will use the local -priv user created for Privilege Elevation: **aduser1@domain.test** will log into the agent as itself and do privilege elevation as the local account

localmachine\aduser1-priv with admin privileges granted.



About Glob Expressions

Glob pattern matching is text matching– for example, if you do a glob pattern search for "app" it returns anything with the exact name of "app." Most of the time people use glob pattern matching in Unix shells or the Windows command window.

The glob standard gives special meaning to a few characters:

Glob Character	Description	Example Pattern	Example Results
* (asterisk)	Matches any number of characters, including zero	`app\*`	application, apple, app
		`b\*d`	bad, bud, bid, bGd, blood, burgundy's last spud
? (question mark)	Matches any one character	`b?d`	bad, bud, bid, bGd
`[ ]` (brackets)	Can contain any number of characters and matches exactly one character if it's contained between the brackets.	`the\*brown\*f?x j[au]\*`	the quick brown fox jumps, the sly, silly brown fox jabbed

For the complete documentation for the glob standard, see https://man7.org/linux/man-pages/man7/glob.7.html.

About Regular Expressions

Regular expression matching is similar to glob pattern matching but allows for more complex patterns. Regular expressions are useful for cases where you want to be more precise or strict with what the expression matches.

For example, consider if you restrict access to commands according to the glob expression vi /etc/ssh/*conf*. This pattern is too generous because users can still run a command such as vi /etc/ssh/../tinyproxy/tinyproxy.conf.

To prevent these kinds of workarounds, you can use regular expressions to more precisely define the matching pattern.

Regular expressions use the following special characters:

- ^ (caret) "anchors" to the start of a line, thus ^foo will only match if "foo" is the first thing found on a text line
- $ (dollar sign) "anchors" to the end of a line, thus foo$ will only match if "foo" are the last three characters on that line
- . (period) matches any one character (like ? in glob)
- ? (question mark) will match exactly zero or one occurrences of the character before it (for example: fa?o will match fao or fo)
- * (asterisk) will match the previous character zero or more times (for example: fa*o will match fo, fao and faaaaaao)
- + (plus sign) will match the previous character at least once and possibly more (for example: fa+o will match fao and faaaaaaaao but NOT fo)
- `.*` (period asterisk) is the same as the bare asterisk * in glob patterns
- `[ ]` (brackets) can surround "ranges" of explicitly enumerated characters (`[aoeui]` for all vowels), implied ranges (`[a-z]` for all lower-case letters from a to z or `[0-9]` for all numerals from zero to nine). You can combine ranges with ?, * and + to match certain repeats of specified ranges.

Our service uses PCRE (Perl Compatible Regular Expressions). For the full documentation, see http://www.pcre.org/original/doc/html/.

Privilege Elevation Workflow

Privilege elevation workflow provides a way for a user to request access to commands that require elevated privileges when the user doesn't already have that access. After the user submits a request, one or more approvers can grant or deny access. If the request is granted, the user can then operate privileged commands on the specified system for the specified time frame.

Here's the overall process for using the privilege elevation workflow:

1. "Enabling Privilege Elevation Workflow" on the next page, either for a system or for all systems (global).
2. "Requesting Privilege Elevation Access" on page 104.
3. "The Access Request Process" on page 106.
4. If granted, the user has "Privilege Elevation Permissions" on page 107 on the affected system.

> **Note:** For privilege elevation workflow activity, the events in the Activity log show that commands were run without an authentication challenge when in fact the user was challenged with additional authentication requests when running the command after the workflow request is approved.

For information about privilege elevation in general, such as requirements, see "Working with Privilege Elevation" on page 90.

Enabling Privilege Elevation Workflow

You can enable privilege elevation workflow either for a system, all systems, or both. If you enable privilege elevation workflow for a system and all systems, the service uses the approver list specified on the individual system.

To Enable Privilege Elevation Workflow on an Individual System

1. Go to **Resources** > **Systems**, and then select the desired system.
2. Click the **Workflow** tab.
3. Select **Yes** for the **Enable Privilege Elevation Request Workflow** option.
4. Specify who can approve the requests:
   a. Click **Add**.
   b. In the drop-down list, select one of the types of accounts:
      i. **Requestor's Manager**: For this approver type, the user's manager will be the approver. Also specify what the recommended action is if the user has no manager defined in the system – the options are:
         i. **Automatically approve**: If the user requesting access doesn't have a manager, the service automatically approves all requests.
         ii. **Automatically deny**: If the user requesting access doesn't have a manager, the service automatically rejects all requests.
         iii. **Route to user or role:** If the user requesting access doesn't have a manager, you can select a specific user or role to be the approver. Click **Add** and search for the desired role or user. Select the desired account and click **Add**.

         Click **Add** to add the specified selection to the list of approvers.
      ii. **Specified user or role**: Here you add the specific user or role who will be the approver. Click **Add** and search for the desired role or user. Select the desired account and click **Add**.
   c. If you've specified more than one approver, click and drag the approvers so reflect the order of priority.

   Each approver must approve the request.
5. Click **Save**.

To Enable Global Privilege Elevation Workflow

1. Go to **Settings** > **Resources** > **Global Workflow** > **Privilege Elevation Workflow** and select the **Enable workflow for privilege elevation requests on all systems** option.
2. Specify who can approve the requests:
   a. Click **Add**.
   b. In the drop-down list, select one of the types of accounts:
      i. **Requestor's Manager**: For this approver type, the user's manager will be the approver. Also specify what the recommended action is if the user has no manager defined in the system – the options are:

i. **Automatically approve**: If the user requesting access doesn't have a manager, the service automatically approves all requests.

ii. **Automatically deny**: If the user requesting access doesn't have a manager, the service automatically rejects all requests.

iii. **Route to user or role:** If the user requesting access doesn't have a manager, you can select a specific user or role to be the approver. Click **Add** and search for the desired role or user. Select the desired account and click **Add**.

Click **Add** to add the specified selection to the list of approvers.

ii. **Specified user or role**: Here you add the specific user or role who will be the approver. Click **Add** and search for the desired role or user. Select the desired account and click **Add**.

c. If you've specified more than one approver, click and drag the approvers so reflect the order of priority.

Each approver must approve the request.

Requesting Privilege Elevation Access

You must have at least View and Agent Auth (login) access to a system in order to request privilege elevation access.

Note: After you request privilege elevation access, you might need to complete another MFA authentication challenge-- depending on how authentication profiles are configured).

To Request Privilege Elevation Access from a Windows System

1. Log in to the Windows system and try to run a privileged operation (for example, open a PowerShell window as Administrator).

   The Windows User Account Control displays with a message saying that you're not authorized to run with privilege and asks you if you want to submit a workflow request.

2. Select the type of workflow request:

   - **Temporary**: You specify when you want your access to begin by specifying how long after the request is approved (in minutes), how long you want your access to last (in minutes), and you can also enter a relevant ticket number (if applicable).
   - **Windowed**: You specify a start and end date and time during which you want to have access. You can also enter a relevant ticket number (if applicable).
   - **Permanent**: You can also enter a relevant ticket number (if applicable).

     Click **Yes** to continue.

     The service forwards your request.

To Request Privilege Elevation Access From a Linux System

1. Log in to the Linux system and try to run a privileged operation (for example, try to run sudo).

   The Linux system displays a message saying that you're not authorized to run with privilege and asks you if you want to submit a workflow request.

2. Enter **Y** and press **Enter** to submit a workflow request.
3. Enter a reason for the request and press **Enter**.

   You don't have to enter a reason, but it can be helpful to enter additional information (for example, a link to a ticketing system).
4. If your organization requires a support ticket, enter it and press **Enter**.

   If not, just press **Enter**.
5. Enter the number for the type of workflow request and then press **Enter**:
   - **1- Permanent**: You can also enter a relevant ticket number (if applicable).
   - **2- Windowed**: You specify a start and end date and time during which you want to have access. You can also enter a relevant ticket number (if applicable).
   - **3- Temporary**: You specify when you want your access to begin by specifying how long after the request is approved (in minutes), how long you want your access to last (in minutes), and you can also enter a relevant ticket number (if applicable).

     The service forwards your request.

To Request Privilege Elevation Access on a Windows or Linux System from the Admin Portal

1. In the Systems view of the Admin Portal, right-click the desired system and select **Request Privilege Elevation**.

   If you're in the system details page, go to the Action menu and select **Request Privilege Elevation**.

   The Request Privilege Elevation Permission dialog box displays.
2. Enter a reason message. The text box has the following prompt message automatically started for you: "I need to run the requested commands with privilege because..."
3. Select the type of workflow request:
   - **Temporary**: You specify when you want your access to begin by specifying how long after the request is approved (in minutes), how long you want your access to last (in minutes), and you can also enter a relevant ticket number (if applicable).
   - **Windowed**: You specify a start and end date and time during which you want to have access. You can also enter a relevant ticket number (if applicable).
   - **Permanent**: You can also enter a relevant ticket number (if applicable).
4. Select the command listing to grant access to it.
   - To grant access to all commands, select **All Commands**.
   - To grant access to specific commands, select **Specific Commands**.
   - To grant access to all sets of commands, select **Command Sets**.

Note: If **Specific Commands** or **Command Sets** are selected, you will be presented with the option to **Add** items to the request based on the selection above. The **Search Command** or **Application** screen displays so that you can search for **Specific Commands** or **Command Sets**.

```
Click __Submit__ to continue.

 The service forwards your request.
```

The Access Request Process

Here's what happens after you submit a request:

The Service Sends an Email to the First Approver

The service sends an email to the approver listed first, indicating that privilege elevation request is pending. The email doesn't include some of the request details, such as requestor, system name, the reason, and a link to the request in the Admin Portal.

The Request Appears in the Admin Portal

The approver can view the request in the Admin portal under: **Access** > **Requests** . The request includes the details pertaining to the request and type of access requested (temporary, windowed, or permanent).

To Approve or Reject a Workflow Request

1. To approve or reject a workflow request, you can either follow the link from the request email or navigate to the **Access** > **Requests**.

   In order to approve a workflow request, you need at least the Privileged Access Service User administrative right.

   Here, you can do the following:

   - **Approve**: The approver first in the list may adjust access request (temporary, permanent, or windowed) and start/end times of temporary and windowed requests.

     If the user has requested access to a command that is affected by more than one defined privileged elevation command, then the one with the highest priority is selected.
   - **Reject**: Specify a reason that you're denying the request.

     Note: If there is more than one approver, after the first approver has approved the request, the service sends the next approver on the list an email as described above and they can approve or reject the request. If an approver is a role, any member of the role may approve or reject the request.

The requestor and approver can also view the request under **Access** > **Request**.

Approval and Rejection Email Information

The following information is included in approval and rejection emails:

Approval email: After the final approver approves a request, an email is sent to the requester with the following:

- System name
- Ticket
- Request types:

- For temporary and windowed assignments: the start/end time (which may have been adjusted from original request)
- For permanent assignments: assignment type
- List of persons who approved and rejected the request

Rejection email: When any approver rejects a request, the service sends an e-mail to the requestor with the following information:

- System name
- Ticket
- List of persons who approved and rejected the request
- Reason for rejection
- A link to the request

Privilege Elevation Permissions

If your request is approved, the Privilege Elevation tab lists your account. If you have temporary access, the page displays the start and ending timestamps.

As with any other permission, an administrator may remove the permission assignment at any time.

Known Issues

Timestamps in the cloud client logs are based on UTC (CC-63703).

Logging in with an Offline Passcode

If an enrolled system isn't currently connected to your network you can log in to it using an offline passcode. You can get the offline passcode either from the Admin Portal or from the Delinea mobile application.

You must have the Offline Rescue permission on a system in order to retrieve the offline passcode.

If your mobile device is also offline, you can still get the offline passcode if it's been fewer than 24 hours since the you last retrieved an offline passcode from the mobile app. If it's been 24 hours or more since you last retrieved an offline passcode from the mobile app, you'll need to get the offline passcode from the Admin Portal.

Note: Mobile offline passcodes are available for both Windows and Linux systems.

To Log In To An Offline System With A Mobile Passcode (Windows Only)

1. In the system's login screen, try to log in with your username.

   The system will prompt you for the OTP (one time password).
2. In the Delinea mobile app, navigate and open your enrolled system.
3. In the screen for your system, click **Offline Passcode**.

   A screen displays your passcode.
4. Enter the offline passcode in the OTP screen on your system.
5. Enter your account password to gain entry into the system.

To Log in to an Offline System with a Passcode from the Admin Portal

1. In the system's login screen, try to log in with your username.

   The system will prompt you for the OTP (one time password).
2. In the Admin Portal, navigate and open the page for your enrolled system.
3. From the Actions menu, click **Show Offline Passcode**.

   A screen displays your passcode.
4. Enter the offline passcode in the OTP screen on your system.
5. Enter your account password to gain entry into the system.

Using Delegated Machine Credentials

During enrollment of a computer to the service, the computer communicates with Privileged Access Service by using its own authentication credentials in the background. You can make use of those same computer or machine credentials to call APIs against your tenant. Using the computer credentials simplifies the authentication process for your automation needs and provides a more secure, contained approach to privileged access. This feature of brokering the computer's trusted credentials without granting direct access to them is called *delegated machine credentials* or DMC.

By using delegated machine credentials, you don't have to set up another OAUTH2 client application and an associated service account with yet another password to manage and so forth. Doing it this way is both more secure and easier to automate.

For example, a DevOps administrator can now automate the creation of temporary computers that run specific workloads and enable those computers to have access to a vaulted secret that they need to run those workloads. A developer can use delegated machine credentials with microservices to authenticate to each other, without having to create and manage service accounts and their credentials.

The main benefits of using delegated machine credentials are as follows:

- Limit the proliferation of service accounts:

  With traditional application to application password management (AAPM), you have to create an OAUTH2 client application and the partner service account, delegate the appropriate permissions, and then embed the client/secret so that the application can call APIs. That set of tasks is per workload.

  With DMC, you can leverage the machine identity and have workloads interact with Delinea PAS using the machine's credentials, thereby reducing the number of service accounts and administrative overhead considerably.
- Use delegated machine credentials in your automation framework:

  You can incorporate client installation, enrollment, and delegation at the point when you initialize your workload systems, thus allowing you to make Delinea PAS a standard part of your DevOps pipeline.
- Reduce your risk:

  You can scope API access for the machine credentials at the individual workload level, so that you give each workload just enough access.

To use Delegated Machine Credentials (an Overview)

1. Set up an enrollment code with preassigned roles and grant the desired permissions to those roles. For details, see Adding systems using enrollment codes.

   The machine account will get the set of permissions granted by the pre-assigned roles.
2. Download and install the Cloud Client for Windows or Cloud Client for Linux in one of the following ways:
   - Manually download the client software. For details, see "Downloading and Installing the Cloud Client for Windows" on page 45:
     - (Windows) Install the Cloud Client for Windows using the wizard. For details, see "Installing and Enrolling the Cloud Client for Windows Interactively" on page 45.
     - (Windows) From a command line, perform a silent install. For details, see "Installing and Enrolling the Cloud Client for Windows Silently" on page 48.
     - (Linux) From a terminal window, install the package. For details, see "Installing the Cloud Client for Linux Package" on page 54.
   - Using AWS or Azure, run scripts to download and install the client. For details, see "Using Sample Scripts for AWS and Azure" on page 42.
3. Enroll a computer and enable delegated machine credentials (DMC) when enrolling, either from the client wizard or command line. For details, see "Enrolling a Computer and Enabling Delegated Machine Credentials" below.

   Note: You must enable DMC at the time of enrollment. If you don't, you have to unenroll and re-enroll with the DMC feature enabled.
4. Configure your applications, scripts, or workloads to call Delinea PAS APIs by referencing the delegated machine credentials. For details, see "Using Delegated Machine Credentials To Call an API" on the next page.

Enrolling a Computer and Enabling Delegated Machine Credentials

After you finish enrolling a computer with delegated machine credentials, you'll see the following in the Admin Portal:

- In the System information, the Client Profile tab lists the DMC feature as enabled.
- In the Users list, the machine account is listed under "All Users" and "All Service Users."

For details about client commands and their parameters, see "Using Cloud Client Commands" on page 111.

For more information about enrolling, see "Installing and Using the Cloud Client for Windows" on page 41 and "Enrolling and Managing Computers Using the Cloud Client for Linux" on page 53.

To Enroll the Computer Interactively and Enable Delegated Machine Credentials on Windows

1. Run the Windows client installer program.
2. On the enrollment page, specify the enrollment code and tenant URL.
   - If you want to enable all client features, don't enter any additional options.

     Information about the other available client features are listed in the information about client commands.

- If you want to enable DMC only, enter "-F DMC" in the additional option field.

  If you'd prefer, you can exit the wizard without specifying any enrollment information. You'll need to later run the cenroll command to enroll the system.

To Enroll The Computer From The Command Line And Enable Delegated Machine Credentials on Windows or Linux

- In a command line window, run cenroll with the following parameters:

```
cenroll -c \<*enrollmentcode*\> -t \<*tenantURL*\> -F dmc -d
[*scopename*:*scopedefinition*]
```

  - Specify the enrollment code with the -c option
  - Specify the entire tenant URL with the -t option
  - Specify -F DMC to enable delegated machine credentials.
  - Optionally, specify the -f option to force enrollment. Doing this can be useful in cases where you have already unenrolled a system without deleting it.
  - Optionally, you can specify the -d option to define an API scope, which defines which APIs are allowed to be called by this machine credential with a scope name and a regular expression. You can also later set the API scope in the system's Client Profile tab.

```
For example, you can specify -d pwd:.+password to define a scope named pwd that
allows any APIs that end in the word "password."
After the enrollment completes, the command displays a message listing the enrollment
parameters.
```

To Unenroll A Computer

- From the command line, run cunenroll. For which specific options to run with cunenroll, see the command line help.

  You can verify that the computer unenrolled successfully either by running cinfo or by checking the system information in the Admin Portal. If you unenroll with the -md option that also deletes the system, then you won't see the system in the list. If you unenroll with the -m option, then you will still see the system listed but there won't be an agent version under the system name nor in the Client Profile.

Using Delegated Machine Credentials To Call an API

Your automation scripts or applications can reference the delegated machine credentials for API calls to Delinea PAS directly or by using the Delinea command line interface (Delinea CLI). For details about APIs, please visit the developer portal.

The examples below use the Delinea command line utility to call the APIs just so that you can see what the API calls might look like. The full instructions are at https://github.com/centrify/centrifycli/wiki/Centrify-CLI:-Centrify-Command-Line-Interface.

To use Delegated Machine Credentials to Call an API using the Delinea Command Line (CCLI)

1. In a command line window, call the desired API with the delegated machine credential:

   ```
   ccli -m [-ms \<apiscope\>] -url \<tenanturl\> \<apiendpoint\> [-f \<jsoninputfile\>]
   ```

   - -m specifies the command line to use machine credentials
   - -ms specifies the API scope and references a scope that you've already defined in the Client Profile. For example, -ms pwd calls an api scope named pwd.
   - -url specifies the tenant URL
   - specify the API endpoint, such as /servermanage/checkoutpassword
   - -f specifies a JSON file, if the API takes an input

     You can have multiple scopes defined, such as a scope for reading secrets and another scope for updating secrets. You can share the read scope with many users but only share the update scope with a handful of administrators.

     So, here's what a full API call might look like, as an example:

     ```
     ccli -m -ms pwd -url https://abc0123.my.centrify.net /servermanage/checkoutpassword -
     j "{'ID':'abcdefgh-1234-ijkl-56789mnopqrs'}
     ```

Using Cloud Client Commands

This section covers commands that you can use on systems where you have installed the Cloud Client. Most commands work the same on Windows and Linux; any differences for operating systems are noted. For details about each command, click the command name to go to the relevant section.

Note: Each command generates a log file at `/var/log/` (Linux) or `C:\ProgramData\Centrify\Logs` (Windows).

Command	Is root or administrator privilege needed?	Description
"cdebug" on the next page	YES	Use the `cdebug` command to control and check the logging detail level. You can also empty the log file as part of your log rotation process.
"cdelaccount" on page 114	YES	Use the `cdelaccount` to delete the domain, database, or local account from Delinea PAS. In order to use this command, the system must have the AAPM feature enabled.
"cdiag" on page 115	YES	Use the `cdiag` command to check configuration settings to diagnose any potential issues with the Cloud Client

Command	Is root or administrator privilege needed?	Description
"cedit" on page 116	YES if you're editing or resetting parameter values	Use the `cedit` command to view, edit, or reset specific Cloud Client configuration parameters.
"cenroll" on page 116	YES	Use the `cenroll` command to enroll the system into Delinea PAS and thereby add the new vaulted system to Delinea PAS.
"cflush (Linux only)" on page 124	YES	You use the `cflush` command on Linux systems to update the local cache of users and groups that have been authenticated by Delinea PAS.
"cgetaccount" on page 125	YES	Use the `cgetaccount` command to retrieve and use the stored password for a domain, database, or managed local account from Delinea PAS. In order to use this command, the system must have the AAPM feature enabled.
"cinfo" on page 126	YES only for the `-H` and `-t` options	Use the `cinfo` command to display detailed and diagnostic information about the local system's configuration in Delinea PAS.
"creload" on page 128	YES	Use the `creload` command to force the client to reload configuration properties after you've changed them using cedit.
"crotatepasswd" on page 129	YES	Use the `crotatepasswd` command to rotate the password for the specified account, such as for a domain, database, or a system account. In order to use this command, the system must have the AAPM feature enabled.
"csetaccount" on page 129	YES	Use the `csetaccount` command to create or update a vaulted privilege account in Delinea PAS for the specified local account. In order to use this command, the system must have the AAPM feature enabled.
"cunenroll" on page 131	YES	Use the `cunenroll` command to un-enroll a vaulted system from Delinea PAS.

cdebug

Use this command to control and check the logging detail level. You can also empty the log file as part of your log rotation process.

Log files are located at `/var/log/cagent.log` (Linux) or `C:\ProgramData\Centrify\Logs` (Windows).

Root or Administrator privilege required? Yes

Usage:

```
cdebug [on | off | clear | status | set <debug_level>
<debug_level> can be TRACE, DEBUG, INFO, WARN, ERROR, DISABLED
```

Command option	Description
`on`	Turns on detailed logging activity. Essentially, this is the same as setting the debug level to DEBUG.
`off`	Turns off detailed logging activity. Essentially, this is the same as setting the debug level to INFO.
`clear`	Empties the current log file and triggers log rotation for the cagent.log file. The client archives the existing log file as cagent-<timestamp>.log.gz and logging starts again from a newly empty cagent.log file. The client also runs the clear command automatically in the background so that log files don't become too large.
`status`	Checks to see whether detailed logging activity is turned on or off
`set <debug_level>`	Sets the level of detail that the client outputs to the log. Your choices are: `TRACE`: Includes trace level messages in addition to what's included with the DEBUG log level. Trace level messages are a step-by-step listing of every action taken; anything that can be logged is captured. Using this log level can help with troubleshooting, but be aware that the log file can get large quickly and system performance may be slower. Delinea recommends that you use this log level only when requested by Delinea Support. `DEBUG`: Debug, informational, warning, and error messages. Use this log level for most troubleshooting situations. Be aware that the log file can get large. Delinea recommends that you use this log level only when requested by Delinea Support. `INFO`: Informational, warning, and error messages. This is the default log level. `WARN`: Warning and error messages `ERROR`: Error messages only `DISABLED`: This option turns off any client logging.

Examples:

```
PS C:\Users\administrator.cloud> cdebug set TRACE
    Debug logging is on. Verbose tracing is on.
```

```
PS C:\Users\administrator.cloud> cdebug status
    Debug logging is on. Verbose tracing is on.
```

cdelaccount

The `cdelaccount` command deletes the domain, database, or managed local account from Delinea PAS. The local account remains intact. After you remove an account from Delinea PAS, you can't check out the password or use Delinea PAS to rotate the password.

In order to use this command, the system must have the AAPM feature enabled.

Note: If you delete an account from Delinea PAS, you must manage the password yourself for the local account. It's recommended that you either save or copy the password manually or change the password after you've deleted the account.

Root or Administrator privilege required? Yes

Usage:

`cdelaccount [-hsVv] [-u, --username __username__] \<account\>`

Command option	Description
`-h --help`	Displays the command help
`-s, --silent`	Specifies that no confirmation will be asked, and the account password will not be displayed.
`-u, --username`	Specifies the administrative user that is used to delete an account . If you specify this parameter, you don't have to run this command as an administrative user. The service will prompt you to enter the password for the specified username.
`-V, --verbose`	Displays the debug information for each operation.
`-v, --version`	Displays the version information.

Examples:

```
# cdelaccount frodo
Caution: Deleting an account means we will no longer know the password. You must make note
of it.
Continue to proceed will make the password available and commit the deletion.
Do you want to proceed? (y/n) [n]: y
Getting account password before deletion...
Password for frodo: OneRingToRuleThemAll%#
Account deleted. Save the password to avoid account lockout.
```

cdiag

Use the `cdiag` command to check configuration settings to diagnose any potential issues with the Cloud Client. The `cdiag` command checks the connection between the client and the platform and also checks if system settings such as PAM or NSS are configured correctly on Linux clients when corresponding features are enabled. You can run this command before, during, or after enrollment.

Run the `cdiag` command if the Cloud Client has any expected functionalities that aren't working, for example.

Note: On Windows, this is a PowerShell script.

Root or Administrator privilege required? Yes

Usage:

```
cdiag -t __tenanturl__ [-dpnV]

cdiag -t __tenanturl__ -v

cdiag -t __tenanturl__ -h
```

Command option	Description
`-t, --tenant url`	Specifies the customer-specific URL of the Delinea PAS. If the system is currently enrolled, this option can be omitted; the URL specified during enrollment will automatically be used. If the system is not enrolled, this option is mandatory. If the system isn't enrolled yet, this option is required.
`-d, --deployment [cloud|on-premise]`	Specifies the deployment type of Delinea PAS. The cdiag command does a different check and troubleshooting according to the deployment type. If you don't specify this option, cloud is the default.
`-p, --http-proxy proxy-url`	Specifies the HTTP proxy URL used by the machine.
`-n, --noreport`	Does not generate a report file.
`-V, --verbose`	Displays the debug information for each operation.
`-v, --version`	Displays the version information.
`-h, --help`	Displays the command help.

Examples: `cdiag -t abc1234.my.centrify.net`

cedit

You can use the `cedit` command to view, edit, or reset specific Cloud Client configuration parameters. For details about which parameters you can edit, see "Customizing Cloud Client Parameters" on page 73.

Root or Administrator privilege required? Yes if you're editing or resetting a parameter value.

Usage:

```
cedit [-hlqv] [-g <key>] [-r <key>] [-s <key>:<value>]
```

Command option	Description
`-g, --get=<key>`	Gets the parameter value.
`-h, --help`	Displays the command help.
`-l, --list`	Lists parameters that are explicitly set.
`-q, --quiet`	Does not display any information.
`-r, --reset=<key>`	Resets the specified parameter value to the default value.
`-s, --set=<key>:<value>`	Sets a parameter value.
`-v, --version`	Displays the version information

Examples:

```
PS C:\Users\administrator.cloud> cedit -l
                FeatureAAPMEnabled: true
                FeatureAgentAuthEnabled: true
                FeatureDMCEnabled: true
                LogLevel: TRACE
                ProxyURL: http://xx.xx.xx.xx:8080
                ServiceURI: https://abc1234.my.centrify.net/
                agent.tcprelay.proxy: http://xx.xx.xx.xx:8080

PS C:\Users\administrator.cloud> cedit -s LogLevel:WARN
                Parameter successfully updated.

PS C:\Users\administrator.cloud> cedit -g LogLevel
                WARN
```

cenroll

Use the cenroll command to enroll the system into Delinea PAS and thereby add the new vaulted system to Delinea PAS. You can also use the cenroll command to update a profile of an existing system that's already enrolled.

In general, the required parameters are:

- `--features`
- `--tenant`
- either `--code` or `--username` (an authentication mechanism —- either an enrollment code or a user with the "System Enrollment" administrative right in Delinea PAS)

Parameters that you might use frequently are:

- agentauth permission to be assigned to a role (`-l`)
- Proxy configuration (`-p`)
- Connector assignment (`-S Connectors:value`)
- Suffix for the hostname in Delinea PAS (`-x`)

Root or Administrator privilege required? Yes

Usage:

```
cenroll [-fhVv] [-a <IP/DNS name>] [-C] [-c <code>] [-F value] [-l<role1>
[,<role2>...,<roleN>]] [-n <name>] [-N <name>] [-O <key:value>] [-o <file>] [-p
<proxyURL>] [-P [user:|role:]<name>:<right>[,<right2>,...,<rightN>]] [-S <key:value>] [-s
<file>] [-t<url>] [-u <username>] [-w <role>] [-x <suffix>] [-Z <set1>[,<set2>...,<setN>]]
```

Command option	Description
`-a`, `--address=<IP/DNS name>` IP address or DNS name of this computer.	Specifies the IP address or DNS name of this computer. The value returned by hostname is used if this argument is not supplied. If a system has multiple network adapters, you can use this option to specify where to direct network traffic from Delinea PAS. By default, if a windows machine is domain joined, then it uses the fqdn (myhost.domain1.net). In some situations, you may want to specify an IP address instead of the hostname for security and network control purposes.
`-C`, `--css`	Enables the CSS Extension for the Cloud Client. By enabling this extension, you can make sure that workflow requests aren't delayed due to Active Directory synchronization schedules. This extension works for Server Suite Agent versions 5.8.0 and later.

Command option	Description
`-c, --code=<code>`	Specifies the enrollment code to use to enroll this computer in the Delinea PAS This option is required, or you must specify a user with "System Enrollment" permission. If the enrollment code is assigned to a role, upon enrollment the service adds the computer into that role.
`-d--dmc-scope=<scopename:regex>,<scopename:regex>,...,<scopename:regex>`	Specifies a delegated machine credential scope name and allowed APIs; you specify the allowed APIs as a regular expression. You can specify this option multiple times in a single command statement.
`-F, --features=value <feature1> [,<feature2>,...,<featureN>]`	Configures specific features for this system. You must specify a value for this option. DMC: Specify this option to enabled delegated machine credentials. For details, see "Using Delegated Machine Credentials" on page 108. `AAPM`: Specify this option to enable application-to-application password management. For details, see "Adding computers as systems". `AgentAuth`: Specify this option to enable the Agent Auth permission, which is needed to allow Delinea PAS users who have the AgentAuth permission to log in. For details, see "Enabling Client-Based Login" on page 82. `all`: Enable all client-based features `none`: Don't enable any client features

Command option	Description
`-f, --force`	Forces the enrollment operation. Use this option if the system already exists in Delinea PAS. Forcing an enrollment overwrites all settings, including any AAPM settings, made during csetaccount. If you force an enrollment you will need to run csetaccount again to return to the same AAPM setting as before the enrollment.
`-h, --help`	Displays the command help.
`-l, --agentauth=<role1>[,<role2>...,<roleN>]`	Specifies the roles to which the AgentAuth/login permission is assigned.
`-m, --groupmap=<role name>:<local group>[,<local group 2>,...,<local group N>]`	Configures a mapping between role and one or multiple local groups on the system. For example, the following maps the System Administrator role to two local groups Administrators and Power Users: `cenroll <standard enroll parameters> -m "System Administrator:Administrators, Power Users"` You can specify this option multiple times in a single command statement. >**Note**: Local group mapping is for Windows systems only.

Command option	Description
-n, --name=<name>	Specifies the login name to use for this computer in the Delinea PAS. The value returned by 'hostname' is used if this argument is not supplied. If the --tenant--suffix argument is supplied, the final name of the system will be in the form <name>@<suffix>. Otherwise, the final name will be the form <name>. The value specified here will appear in Resources > Systems in PAS.
-N, --resource-name=<name>	Specifies the name of this computer in Delinea PAS. The value returned by 'hostname' is used if this argument is not supplied. If the --tenant-suffix argument is supplied, the final name of the system will be in the form <name>@<suffix>. Otherwise, the final name will be in the form <name>.
-O, --resource-policy=<key:value>	Specifies resource-specific policies in key-value pairs. If the same policy is configured by this parameter and the --resource-policy-file, the value in this parameter is applied. You can specify this option multiple times in a single command statement.
-o, --resource-policy-file=<file> and the --resource-setting-file,	Specifies a plain text file that contains resource-specific policies stored as key-value pairs. If the same policy is configured by this parameter and resource-policy, the value in resource-policy is applied.
-p, --http-proxy=<proxy URL>	Specifies an HTTP proxy to use for the Cloud Client connection to Delinea PAS. When you specify this option, the client redirects all communication through the proxy address. If the proxy is unavailable, the client status is listed as "disconnected" from the network.

Command option	Description

`-P`, `--resource-permission`
 	
For Active Directory or LDAP groups:
 	
`cenroll -P group: "<group@domain.suffix>":<PAS_permission>`
 	
For Delinea PAS roles:
 	
`cenroll -P <role_name>:<PAS_permission>`
	Specifies the permissions for the system, such as Grant, View, AgentAuth, Offline Rescue, and so forth. You can specify permissions for users or roles. For more details about permissions, see Assigning permissions.
	
	It can be useful to specify permissions at the time of enrollment, but you can set them later in the Admin Portal too. You can specify this option multiple times in a single command statement — when you specify multiple permissions, surround each permission with \". For example:
	`-P \"bugs.bunny@acme.cloud:Grant,View\" --resource-permission "bugs.bunny@acme.cloud:Grant,View"`

Command option	Description
`-S, --resource-setting=<key:value>`	Specifies resource-specific settings in key-value pairs. If the same setting is configured by this parameter and the `--resource-setting-file`, the value in this parameter is applied. To set the domain information, you can specify `DomainName:<domain>` as a setting. You can specify this option multiple times in a single command statement You can view the available resource settings here: developer portal - post_servermanage-updateresourcedeveloper portal - post_servermanage-addresource >**Note**: When supplying a connector resource setting, specify just one connector. If you specify more than one, the last one you specify will be used. For example: `cenroll -f -F all -S Connectors:connector1`
`-s, --resource-setting-file=<file>`	Specifies a plain text file that contains resource-specific settings stored as key-value pairs. If you specify the same parameter in this file and the `--resource-setting` parameter, the client uses the value specified in the `--resource-setting` parameter.
`-t, --tenant=<url>` Customer-specific URL	Specifies the tenant to enroll into. You can use either a space or = between the --tenant and the URL. Here are some examples of the ways you can specify a tenant URL: `--tenant=abc0123.my.centrify.net --tenant abc0123.my.centrify.net --tenant https://abc0123.my.centrify.net --tenant=https://abc0123.my.centrify.net`

Command option	Description
-u, --username=<username>	Specifies the user who will enroll this system into the Delinea PAS You must either specify this option or specify an enrollment code.
-V, --verbose	Displays debug information for each operation.
-v, --version	Displays the version information.
-w, --owner=<role>	Role used to manage this computer in the Delinea PAS.
-x, --suffix=<suffix>	Specifies the suffix to use for the login and resource names for this system.
-Z, --resource-set=<set1>[,<set2>...,<setN>]	Adds the system to the specified resource sets.

Examples:

```
[EXAMPLE: to enroll a system with all features enabled into the specified tenant using an
enrollment code]
[root@mylinux ~]# cenroll --force --features=all --tenant=abc1234.my.centrify.net --
code=PUTTHEENROLLMENTCODEHERE
            Enrolling in https://abc1234.my.centrify.net/ ...
            Centrify agent started.
            Enabled features: AgentAuth, AAPM, DMC
            Enrollment complete.

[EXAMPLE: To add a local computer to the Privileged Access Service using a specified user
account]
[root@mylinux ~]# cenroll --tenant=abc1234.my.centrify.net --user wily@acme --features
aapm,agentauth --agentauth "Authorized Agent Login"


[EXAMPLE: To add the computer using a specific IP address and computer name]
[root@mylinux ~]# cenroll -t abc1234.my.centrify.net -u wily@acme -n rhel9.mydomain.com -a
123.45.67.890


[EXAMPLE: To add the computer and enable all features and use a web proxy]
[root@mylinux ~]# cenroll -F all -f -t abc1234.my.centrify.net -c PUTTHEENROLLMENTCODEHERE
-l linuxadmins -p http://12.3.4.56:8080


[EXAMPLE: To add the computer and enable AAPM ]
```

```
[root@mylinux ~]# cenroll -F AAPM -f -t -abc1234.my.centrify.net -c
PUTTHEENROLLMENTCODEHERE -l linuxadmins


[EXAMPLE: To enroll a computer with username and password instead of an enrollment code]
[root@mylinux ~]#
cenroll -F all -f -t abc1234.my.centrify.net -u  -u pasadmin@example.com -l linuxadmins



[EXAMPLE: To allow the public network access for this computer and to perform periodic
password rotation on the accounts associated with this
computer every 30 days, specify these policies on the command line]
[root@mylinux ~]# cenroll -O "AllowRemote:true" -O "AllowPasswordRotation:true" -O
"PasswordRotateDuration:30"


[EXAMPLE: Alternatively, you could use a text editor to create a "policy.conf" file with
settings:]
AllowRemote:true
AllowPasswordRotation:true
PasswordRotateDuration:30



[After defining the policies in the "policy.conf" file, run the cenroll command and refer
to the policy.conf file:]
[root@mylinux ~]# cenroll --resource-policy-file /tmp/policy.conf


[EXAMPLE: enroll with Use My Account credentials]
cenroll -F agentauth -t tenant> -c <code> -l <agentauth_role> -S CertAuthEnable:true -S
AllowRemote:true  -S Connectors:<name>

[NOTE: Using the cenroll command depends on the user in PAS being a member of a role with
AgentAuth permission. Use My Account will be immediately accessible for Windows enrolled
systems, and then accessible for Linux enrolled systems after MasterSSHKey
download/configuration.]
```

cflush (Linux only)

You use the `cflush` command on Linux systems to update the local cache of users and groups that have been authenticated by Delinea PAS.

User and group information is stored in the local cache so that the client does not need to lookup the information for the next 60 minutes (after it is stored). This command invalidates the information in the local cache such that the client will request the information from Delinea PAS whenever any client application asks for such information.

Because most Linux applications need to look up user or group information, caching such information reduces the need to frequently request the same information from PAS. Caching this information improves performance.

Root or Administrator privilege required? Yes

Usage:

```
cflush [-eV]

cflush -v

cflush -h
```

Command option	Description
-e, --expire	(Reserved for future use)
-V, --verbose	Displays detailed debug information for each operation.
-v, --version	Displays the version information.
-h, --help	Displays the command help.

Examples:

```
[root@mylinux ~]# cflush
        Flushed cagent cache
```

cgetaccount

Use the cgetaccount command to retrieve and use the stored password for a domain, database, or managed local account from Delinea PAS. (You can store accounts either from within the Admin Portal or by using the csetaccount command.) In order to use this command, the system must have the AAPM feature enabled.

Root or Administrator privilege required? Yes

Usage:

```
cgetaccount [-tTsvV] [-t, --lifetime minutes] [-T, --type type ] [-s, --silent] [-u, --username username] [-v, --version] [-V, --verbose] targetname / accountname
```

Command option	Description
-t, --lifetime Minutes	Specifies the password checkout interval (duration), in minutes. The value that you specify must be less than or equal to the account checkout lifetime defined in the target policy. If you specify a value greater than the account checkout lifetime, and error is returned. If you do not specify a password checkout interval (that is, if you do not use this option), a default password checkout interval of one minute is used.
-T, --type Type	Specifies the type of the target to which the account belongs. Valid values are system, domain, or database.

Command option	Description
`-s, --silent`	Retrieves the account password from Delinea PAS without asking for confirmation. The password is not printed to stdout. This option is useful for scripts that need to set a local variable in order to store the returned password.
`-u, --username`	Specifies the administrative user that is used to get an account . If you specify this parameter, you don't have to run this command as an administrative user. The service will prompt you to enter the password for the specified username.
`-v, --version`	Displays the version information.
`-V, --verbose`	Displays information about each step in the password retrieval operation as it occurs. This option can be useful in diagnosing password retrieval problems.
`-h, --help`	Displays usage information for this command.

Examples:

```
[root@mylinux ~]# cgetaccount frodo
            Password for account "frodo" will be checked out. The checkout will be logged
and expire in 1 minute.
            Do you want to continue and display the password? (y/n) [n]: y
            Password for frodo: OneRingToRuleThemAll%#
```

cinfo

Use the `cinfo` command to display detailed and diagnostic information about the local system's configuration in Delinea PAS.

Root or Administrator privilege required? Yes if you're using the --support option

Usage:

```
cinfo [-aADhNoPtTVv] [-C <url>] [-p <proxy URL>]
```

Command option	Description
`-a, --address`	Displays the IP address or DNS name for an enrolled instance in the Delinea PAS.

Command option	Description
-A, --agent-status	Displays the status of the Cloud Client. The possible values are as follows: unknown: The cinfo command failed to check the client status or encountered an unknown error. connected: The client is connected to the Delinea PAS and running well. disconnected: The client is not connected to the Delinea PAS, most likely due to a network connectivity issue. stopped: The client service has been stopped by a system management tool, such as systemctl. starting: The client is in the process of starting and not yet ready for service. disabled: The client has discovered that the related resource has been deleted in the backend, so the client cannot work anymore.
-B, --clientchannel-status	Confirms that the Cloud Client has a connection to Delinea PAS. For example, if the client is connected, the service allows password reconciliation to work. The possible status options are either online or offline.
-C, --connect=<url>	Verifies the availability of the Delinea PAS by connecting to the specified URL.
-D, --tenant-id	Displays the registered customer-specific identifier (tenant ID).
-H, --clientchannel-health	Performs a Cloud Client health check of the client channel, which is the connection between the Cloud Client and Delinea PAS. This option requires Administrator or root privilege.
-h--help	Displays the command help.
-N--resource-name	Displays the resource name for a computer enrolled in the Delinea PAS.
-o--owner	Displays the owner of a computer enrolled in the Delinea PAS.
-p, --http-proxy=<proxy url>	Specifies the HTTP proxy to use in conjunction with the --connect option.
-P, --platform-version	Displays the version of Delinea PAS.

Command option	Description
-t, --support	Generates a support file with diagnostic information. The file location is: /var/centrify/tmp/cinfo_support.tar.gz (Linux) C:\ProgramData\Centrify\support\cinfo_support.<timestamp>.zip (Windows) This option requires Administrator or root privilege.
-T, --tenant	Displays the customer-specific URL for a computer enrolled in Delinea PAS.
-V, --verbose	Displays debug information for each operation.
-v, --version	Displays the version information.

Examples:

```
root@mylinux ~]# cinfo
                Enrolled in:       https://abc1234.my.centrify.net/
                Enrolled as:
                    Service account:  mylinux$@acme.net
                    Resource name:    mylinux
                    IP/DNS name:      10.10.10.1
                    Owner:            sysadmin (Type: Role)
                Customer ID:        ABC1234
                Enabled features:   AgentAuth, AAPM, DMC
                Client Channel status: Online
                Client status:      connected
```

creload

Use the creload command to force the client to reload configuration properties after you've changed them using cedit.

Root or Administrator privilege required? Yes

Usage:

```
creload [-hVv]
```

Command option	Description
-h,--help	Displays the command help.
-V, --verbose	Displays debug information for each operation.
-v, --version	Displays the version information.

Examples:

```
[root@mylinux ~]# creload
```

crotatepasswd

Use the `crotatepasswd` command to rotate the password for the specified account, such as for an account for a domain, database, or a system. If you're rotating the password for a vaulted local account, the password is updated both locally and in the Admin Portal. If the password is currently checked out, you must use the `--force` option to force the password rotation. In order to use this command, the system must have the AAPM feature enabled.

Root or Administrator privilege required? Yes

Usage:

```
crotatepasswd [-fhVv] [-T value] [<target>/]<account>
```

Command option	Description
`-f, --force`	Ignores any password checkouts and force a password rotation.
`-h, --help`	Displays the command help.
`-T, --type=value`	Specifies the type of the target to which the account belongs. Valid values are: system, domain, or database.
`-V, --verbose`	Displays debug information for each operation.
`-v, --version`	Displays the version information.

Examples:

```
[root@mylinux ~]# crotatepasswd frodo
            Rotating password for frodo...
            Failed to rotate password for frodo: Failed to rotate password from identity
platform: The password for this account is currently checked out
[root@mylinux ~]#
[root@mylinux ~]# crotatepasswd --force frodo
            Rotating password for frodo...
            Rotated Password for frodo
```

csetaccount

Use the `csetaccount` command to create or update a vaulted privilege account in Delinea PAS for the specified local account. In order to use this command, the system must have the AAPM feature enabled.

Root or Administrator privilege required? Yes

Usage:

```
csetaccount.exe [-hPVv] [-a <name>|user:<name>|role:<name>] [-d <description>] [-m
<true|false>] [--password <password>] [-p [user:|role:|group:]<name>:<right>
[,<right2>,...,<rightN>]] [-s <set1>[,<set2>...,<setN>]] [--stdin] [-u, --username
username] [-w <enable|disable|default>] [-x <true|false>] <account>
```

Command option	Description
-a, --approver=<name>|user:<name>|role:<name>	Specifies the approver for the account. This parameter applies if privileged account workflow is enabled.
-d, --description=<description>	Specifies the account description.
-h, --help	Displays the command help.
-m, --managed=<true|false>	Specifies whether the account password is managed.
-P, --nopassword	Specifies to not require password input. Use this option to update the account settings without updating the stored password.
--password=<password>	Specifies the account password. If you don't specify this parameter, then you're prompted for the password.
-p, --permission= [user:|role:|group:]<name>:<right> [,<right2>,...,<rightN>] | Specifies the account permissions.	
-s, --set=\set1>[,<set2>...,<setN>]	Specifies one or more sets to add the account to.
--stdin	Reads the user password from stdin instead of an interactive prompt.
-u, --username	Specifies the administrative user that is used to add or update an account. If you specify this parameter, you don't have to run this command as an administrative user. The service will prompt you to enter the password for the specified username.
-V, --verbose	Displays debug information for each operation.
-v, --version	Displays the version information.
-w, --workflow=<enable|disable|default>	Specifies whether privileged account workflow is enabled.
-x, --useproxy=<true|false>	Specifies the account to use as a proxy account.

Examples:

```
[root@mylinux ~]# csetaccount -m true frodo
```

```
Password for frodo:
Account frodo has been successfully vaulted
```

cunenroll

Use the `cunenroll` command to un-enroll a vaulted system from Delinea PAS. Un-enrolling a system means the following:

- Remove the system from Delinea PAS in such a way that any client-based features no longer work on the system (unless you re-enroll the system).
- Unless you specify otherwise, un-enrolling does not completely remove the system from Delinea PAS. Vault functions such as remote access to the system still work. The system displays in Delinea PAS with an unenrolled status.
- The Cloud Client software remains installed on the system. This way, you can re-enroll the system without having to reinstall anything.

To unenroll a system using the `cunenroll` command, you must specify one of the following options:

- `\-m machine credential`
- `\-u user credentials` (the user account must have Grant permission on the system)

To completely remove the system from Delinea PAS, you specify the option `-d`. Using the `-d` option removes the system completely from Delinea PAS and any client-generated accounts. To remove a system from Delinea PAS, you must have the View and Delete permissions.

Root or Administrator privilege required? Yes

Usage:

```
cunenroll [-CdfhmRtVv] [-u value]
```

Command option	Description
`-C`, `--noconf` (Linux only)	Specifies to not update the local configuration upon unenrolling from the Delinea PAS. >**Note**: Please contact Delinea Support before you use this parameter.
`-d`, `--delete`	Deletes this computer account from the Delinea PAS, including all resource information and all associated accounts.
`-f`, `--force`	Forces an unenroll operation locally without connecting to the Delinea PAS.
`-h`, `--help`	Displays the command help.
`-m`, `--machine`	Uses the machine credential to unenroll from Delinea PAS.

Command option	Description
`-R, --restore` (Linux only)	Restores the configuration without unenrolling from Delinea PAS. The `--restore` option restores the PAM/NSS modules configuration so that the Delinea PAS modules are not loaded anymore and the PAM/NSS state back to what it was like it was before enrollment. >**Note**: Please contact Delinea Support before you use this parameter.
`-t, --terminate-user-sessions`	Use this option together with the 'delete' option. If there are any current sessions where user initiated the connection from within Delinea PAS, use this option to terminate all of the sessions. Sessions that were initiated from the command line are not terminated.
`-u, --user=value`	Specifies the administrative user used to unenroll from the Delinea PAS.
`-v, --verbose`	Displays debug information for each operation.
`-v, --version`	Displays version information.

Examples:

```
(This example uses the system's service account in PAS and deletes the system in PAS.
            [root@mylinux ~]# cunenroll --delete --machine
            Successfully Unenrolled.
```

Un-Enrolling a System

When you unenroll a Windows or Linux system from Delinea PAS, you're disconnecting it from the service. Unenrollment does not uninstall the client from the system, and unenrolled systems do continue to display in the list of systems but they display as unenrolled.

You can unenroll a single or multiple systems from the Systems page. You can also right-click a set and unenroll all systems in that set.

In order to unenroll a system from the Admin Portal, you must be assigned to a role that has the System Enrollment administrative right. To remove a system from Delinea PAS, you must have the View and Delete permissions.

You can also unenroll a system from the command line. For details, see "cunenroll" on the previous page.

Note: (Alpine Linux systems only) Before you uninstall the Cloud Client for Linux from an Alpine Linux system, you must unenroll the system first. The Alpine Linux package manager doesn't allow the service to verify that the client is unenrolled from Delinea PAS before uninstalling. If you uninstall the client without unenrolling first, you won't be able to log in to the system anymore.

To Unenroll a System

1. In the Systems page, select one or more systems that you want to unenroll.
2. From the Actions menu, if you selected a single system, choose **System** > **Unenroll**.

If you selected multiple systems, choose **System** > **Unenroll Systems**.

A popup dialog appears for you to verify the unenroll operation.

3. By default, the option to not unenroll any systems that have password reconciliation enabled is selected. You can deselect this option, if desired.
4. Click **Unenroll** to continue.

   If you unenrolled multiple systems, a popup displays to inform you that the operation is scheduled and you'll get an email when the unenrollment is complete for all systems. That email includes a link to the job report.

   Click **Close** to close the popup message and return to the Systems page.

   The unenrolled systems will display in the list of systems as unenrolled and their client profile shows all features are disabled.

   If you run cinfo on the affected systems, the status message will indicate that the system is not enrolled in Delinea PAS. If you want to enroll the system again, you will need to use the -f force option; otherwise, the enrollment will fail with a message indicating that the system already exists in the platform.

Upgrading the Cloud Client

When you need to install a newer version of the Cloud Client, just download and install the newer version. You don't need to uninstall the old version. Also, if the computer is already enrolled, upgrade doesn't impact enrollment.

You can also configure a policy so that the client automatically updates to the latest version. For details, see Enabling client automatic updates.

Introduction to Hyper-scalable Privileged Access Service

The Delinea Hyper-scalable Privileged Access Service (Hyper-scalable PAS) deployment model is an on-site solution where you provide your own servers as part of the infrastructure solution. The infrastructure you choose can be either an internal protected network, a private cloud, or a public cloud instance.

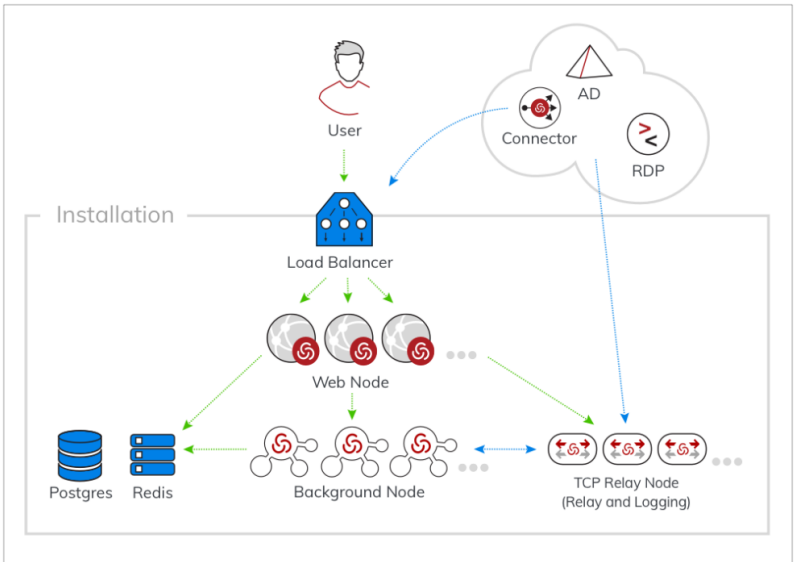
Hyper-scalable PAS uses a scalable approach; each installation includes an unlimited number of Web, Background, and optionally TCP Relay (Relay and Logging) nodes running Privileged Access Service software on a Windows Server operating system. These nodes must be able to communicate with each other and the following additional components that make up the installation (for specific component requirements, see "Prerequisites" on page 146):

- Cache server (Redis)
- Database server (PostgreSQL)
- Load Balancer

Additionally, outside of the cluster, a Management node is required to manage the cluster.

See the following for a run time overview of the Hyper-scalable PAS.

Note: Components with the Delinea icon execute product code provided by Delinea.



Installation Concepts

This installation and configuration guide describes how to install, upgrade, and configure the Hyper-scalable PAS as a solution in a high availability (HA) environment. An installation is the configuration for a specific hostname and certificate that define the site enabled by this Delinea PAS deployment. After you install Hyper-scalable PAS, you use the Admin Portal to add, manage, and access the resources, domains, and databases and the corresponding accounts within the Privileged Access Service. The following concepts provide some context that can be helpful in understanding the overall installation process. For an overview of the installation, see "Installing Hyper-scalable PAS" on page 163.

- Cluster Site Installation

  A cluster installation/site is defined as the configuration of nodes with the Hyper-scalable PAS software package installed. Each installation/site requires a single hostname and certificate to be defined for that particular site. For example, pas.yourcompany.com indicates a particular site installation, with one hostname, matching host certificate, and database server, while company.acme.com would be a different site installation with a different database server and a different host certificate. To create an installation, you need to install and deploy the Hyper-scalable PAS software to the Management, Web, Background, and TCP Relay nodes. During installation you create the deployment package that allows you to easily deploy to specific nodes.

- Deployment

  A Hyper-scalable PAS Deployment is the specific version of the software and configuration used to create node instances. This is created and packaged using Centrify-PAS-NewDeployment. That package is then used to create new nodes, which are associated with that specific Deployment (see the next section, *Deployment Instance*.

- Deployment Instance

  A Hyper-scalable PAS *deployment instance* is a node on a server created using a Deployment package, for example by calling Centrify-PAS-Deploy-WebNode. In addition to Web and Background nodes, you can also deploy the Hyper-scalable PAS software two types of TCP Relay nodes: Logging node and a Relay node.

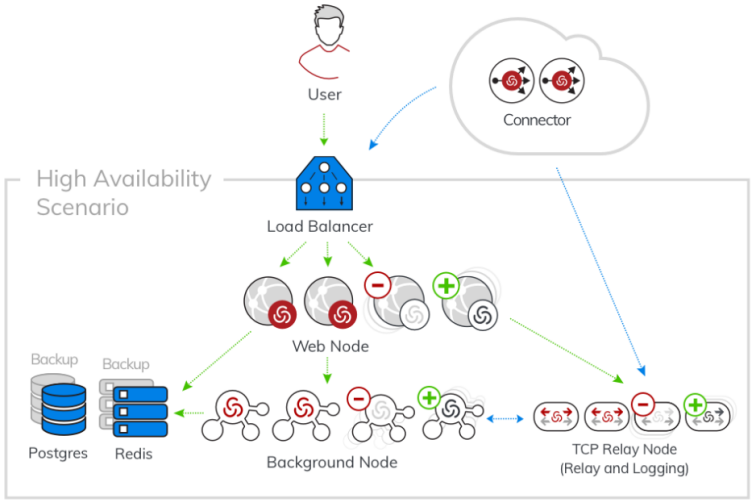
High Availability and Scale

The Hyper-scalable PAS gives you the ability to easily add additional Web and Background nodes to make it a scalable, high availability solution. Generally your solution should include two or more Web, Background, and optionally TCP Relay nodes. For more information, see "Scaling and High Availability" on page 190.

The following additional components that make up your Hyper-scalable PAS solution will also need to be sized to meet your scalability and high availability needs:

- Cache (Redis)
- Database (PostgreSQL)
- Load balancer
- Networking and power infrastructures
- Connector

The following shows how high availability works in Hyper-scalable PAS.



Note: Node monitoring is dependent on your organizations chosen software.

Backup and Disaster Recovery

To ensure uninterrupted service in the event of a major system failure, we recommend maintaining a back up of your configuration and database instances. Maintaining these backups helps to ensure fastest recovery from a system failure. For more information on disaster recovery, see "Backup and Disaster Recovery" on page 208.

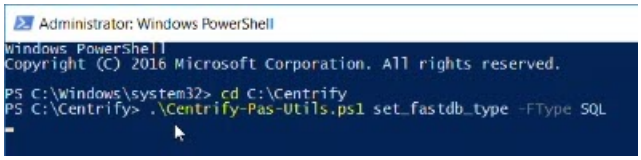
Migrating from PostgreSQL 10/11 to PostgreSQL 14

Updating from PostgreSQL 10 or 11 to PostgreSQL 14 will require the PLV8 extensions to be removed as the PLV8 extensions do not support PostgreSQL 14.

The following steps will walk through how to upgrade from PostgreSQL 10 or 11 to PostgreSQL 14 along with the steps to remove any PLV8 extensions in the PostgreSQL 10/11 database.

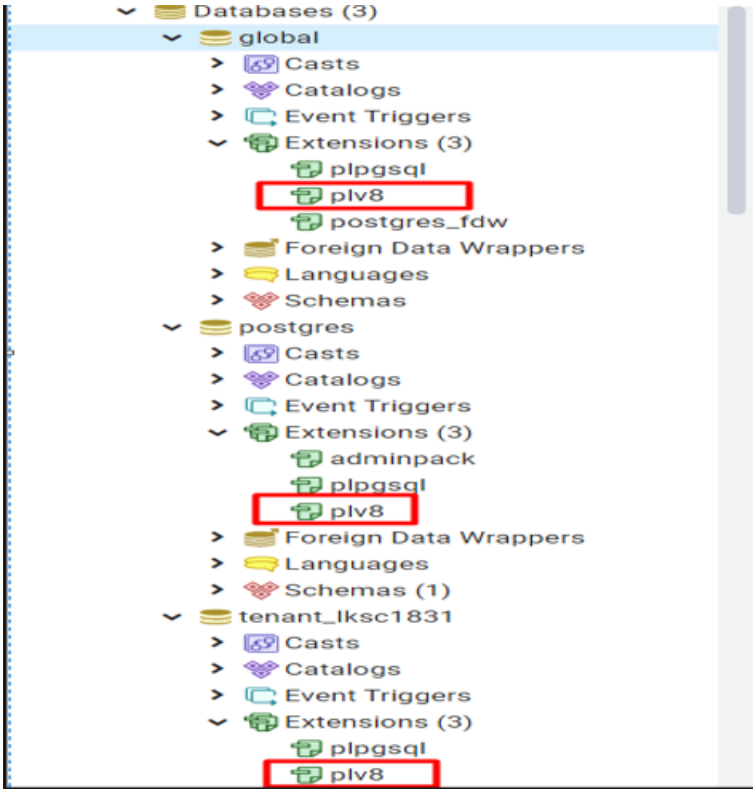
1. Check that the PAS web app is online.
2. Then in Windows PowerShell change the FastDB type to SQL. To do that execute the following as an admin:

```
cd C:\Centrify
.\Centrify-Pas-Utils.ps1 set_fastdb_type -FType SQL
```



> **Note:** After the above has been executed, you will receive a notice stating:
> `Set FastDB Type result: @success=True;`
> This indicates that the FastDB type will successfully change into SQL.

3. Open the **PGAdmin** program.
   a. Select the **Servers** drop down menu by selecting the arrow on the left-hand side. Select the **Databases** drop down menu. The PLV8 extension will need to be deleted from all databases.
   b. Open each database's **Extension** drop down menu to see which ones have PLV8.



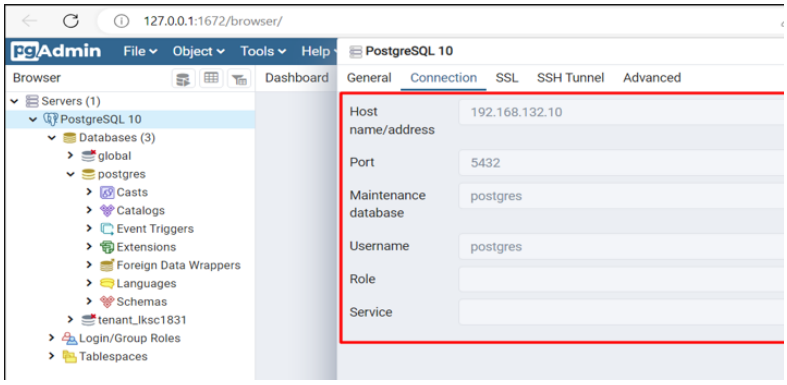
   c. Right-click **plv8** under the database you are deleting it from. Click **Delete/Drop**.

d. Click **OK** when the **Drop Extensions?** pop up appears.

e. Repeat these steps until PLV8 is removed from all databases in **PGAdmin**.

4. In **PGAdmin** under the **Servers** drop down menu, right-click **PostgresSQL 10**. Click **Properties**.

5. Select the **Connection** page. Write down the connection parameters of the PG10/11 server to reuse them for the PG14 server.



6. Download and install PostgresSQL14 here:

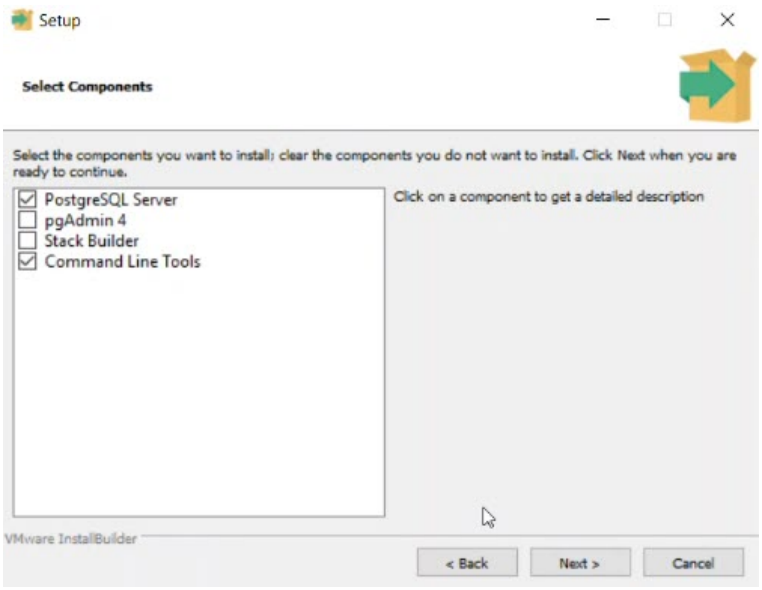
   `https://www.enterprisedb.com/downloads/postgres-postgresql-downloads`

   a. Download PostgreSQL 14.9 by selecting the blue box with a downward arrow under **Windows z86-64** or under **Mac OS X**.

   b. After PostgreSQL14 has successfully downloaded, open **File Explorer** on your computer and select the **Downloads** file. Open the new PostgreSQL 14.9 folder and select **Yes** when prompted to allow the app to make changes on your device.

   c. A **Setup** page will pop up, click **Next** through the **Installation Directory** page. Then on the **Select Components** page install **PostgreSQL Server** and **Command Line Tools**.

   Note: Make sure you unselect **pgAdmin 4** and **Stack Builder** before clicking Next.



d. Click **Next**. On the **Data Directory** page, click **Next**.

e. Add your password to the **Password** page, then click **Next**.

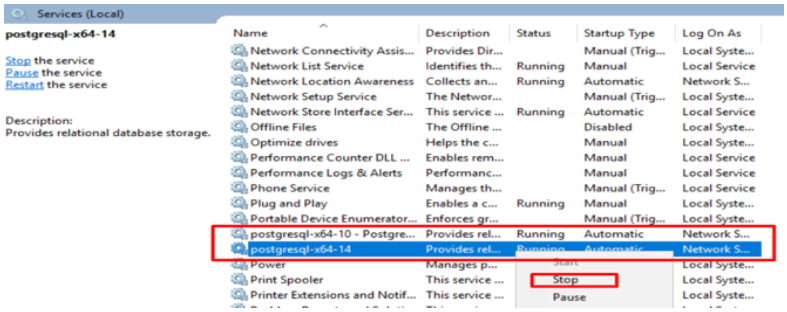
> **Note:** It is best to use the same password you used for PostgreSQL 10.

f. Click **Next** through the following pages:

- **Port**
- **Advanced Options**
- **Pre Installation Summary**
- **Ready to Install**

g. Select **Finish** after Setup has finished installing.

7. Open the**Services** app and stop **PostgreSQL10** and **PostgresSQL14** services by right-clicking on them and selecting **Stop**.



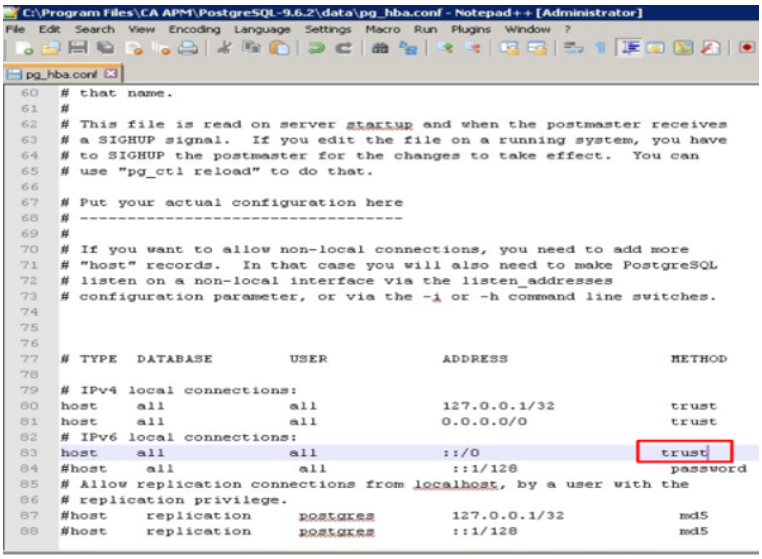
8. Adjust the authentication on PG10 and PG14 by opening the **Command Prompt** app.

a. Open **Notepad** within the app.

b. Select **File** and then select **Open**. Then open:

`C:\Program Files\PostgreSQL\10\data\pg_hba.conf` folder for PG10

c. Record the existing method for `# IPv6 local connections` and temporarily change that method to: `trust`.



d. Save.

e. Open:

`C:\Program Files\PostgreSQL\14\data\pg_hba.conf`

Repeat these steps for PG14.

9. Add a new local user to PostgreSQL by opening **Computer Management**.

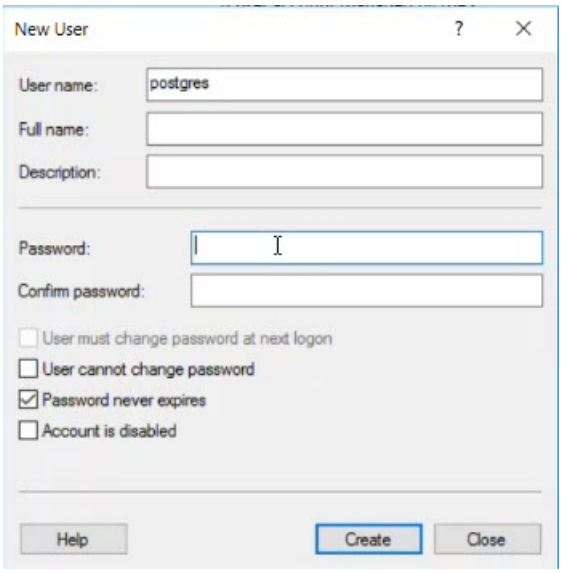
a. Select **Local Users and Groups**, right-click the **Users** folder and select **New User**.

b. For username use: `postgres`.

Unselect the **User must change password at next logon** box. Then select the **Password never expires** box.

c. Use the same password used for PostgresSQL14. Then select **Create**.

> **Note:** If Windows doesn't allow you to create a new user because the password doesn't comply with the password security policy follow this document: https://www.wintips.org/how-to-disable-password-complexity-requirements-on-server-2016/



d. Select **Close**. Then the PostgreSQL user should appear under the **Users** folder.

e. Grant full control to the following folders by navigating to **File Explorer** and searching for the below folders:
   - `C:\Program Files\PostgreSQL\10`
   - `C:\Program Files\PostgreSQL\10\data`
   - `C:\Program Files\PostgreSQL\14`
   - `C:\Program Files\PostgreSQL\14\data`

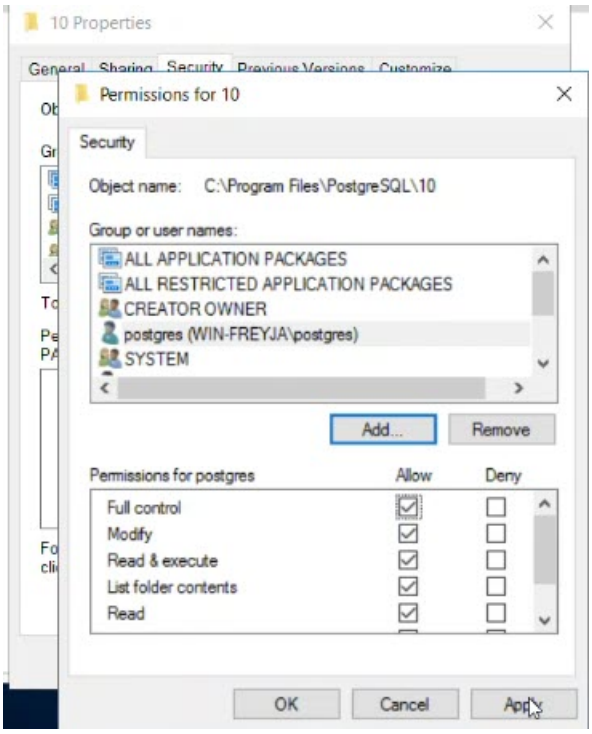
f. Right-click the first folder and select **Properties**.

g. The Properties page will appear, select **Security** and then click **Edit**.

h. Click **Add** then click **Locations** and select **Computer Name** and click **OK**.

i. Click **Advanced** and click **Find Now** and select the PostgreSQL user. Then click **OK**.

j. Select the PostgreSQL user and under **Permission for postgres** select the **Allow** box to the right of **Full Control**.Then click **Apply**.

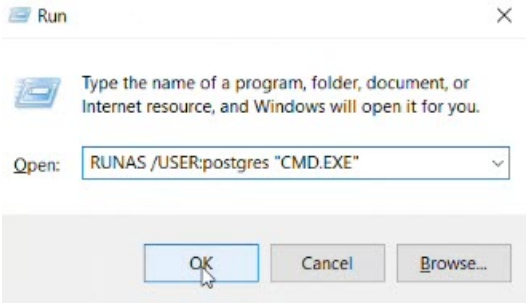


k. Repeat these steps for all 4 folders.

10. Run:

    ```
    RUNAS /USER:postgres "CMD.EXE"
    ```

    Click **OK**.



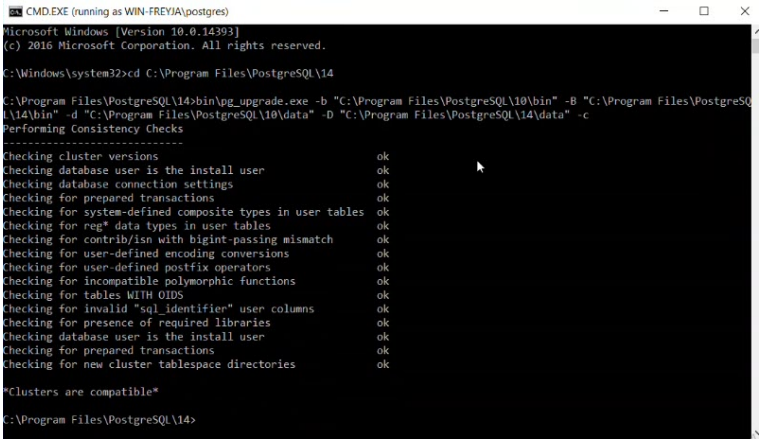
11. Enter the password for PostgreSQL to login as the PostgreSQL user.
12. To run a `db_upgrade` check, change to the PG14 directory by adding:

    `cd C:\Program Files\PostgreSQL\14`.

    a. Add the following to run the `db_upgrade` **check**:

    ```
    bin\pg_upgrade.exe -b "C:\Program Files\PostgreSQL\10\bin" -B "C:\Program
    Files\PostgreSQL\14\bin" -d "C:\Program Files\PostgreSQL\10\data" -D "C:\Program
    Files\PostgreSQL\14\data" -c
    ```

b. All checks should come back as 'ok' showing that the migration from PG10/11 to PG14 will be successful.



c. Run the upgrade using the following:

```
bin\pg_upgrade.exe -b "C:\Program Files\PostgreSQL\10\bin" -B "C:\Program Files\PostgreSQL\14\bin" -d "C:\Program Files\PostgreSQL\10\data" -D "C:\Program Files\PostgreSQL\14\data"
```

d. After the upgrade has completed set the PG10 `pg_hba.conf` back to it's original method instead of `trust` in:

`C:\Program Files\PostgreSQL\10\data\pg_hba.conf`.

(See Step 8 for reference).

13. Replace both **pg_hba.conf** and **postgresql.conf** in:

`Files\PostgreSQL\14\data`

with the files from:

`C:\Program Files\PostgreSQL\10\data`.

> **Note:** You can make copies of the **pg_hba.conf** and **postgresql.conf** in `Files\PostgreSQL\14\data` before you replace them in case you should need to reference them later on. If you do this, copy and paste the two files in PG14 to a new location.

a. Open the folder:

`C:\Program Files\PostgreSQL\10\data` .

Select both **pg_hba.conf** and **postgresql.conf** and copy them.

b. Navigate to the folder:

`Files\PostgreSQL\14\data`.

Paste the copied files into the PG14 folder.

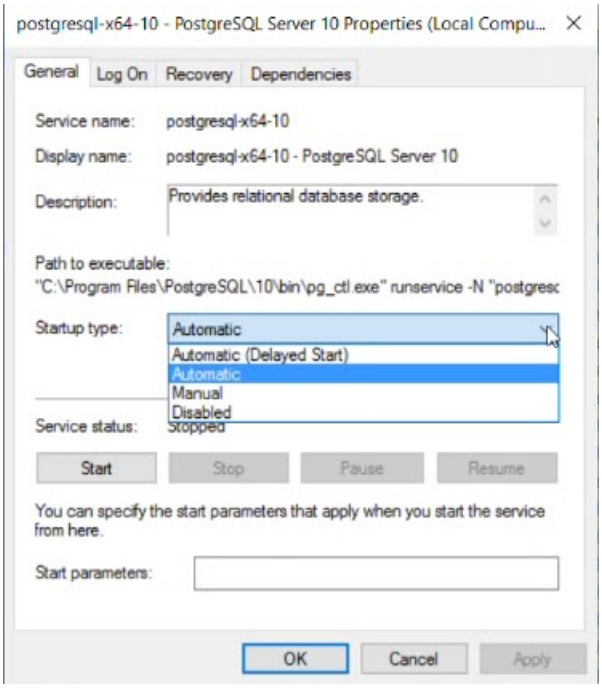
c. Select **Replace the files in the destination**.

14. Set the **Startup type** to **Disabled** for the PG 10 service.

a. Go to the **Services** application.

b. Right-click PostgreSQL 10. Click **Properties**.

c. Change the **Startup type** from Automatic to **Disabled**.



d. Click **Apply** then click **OK**.

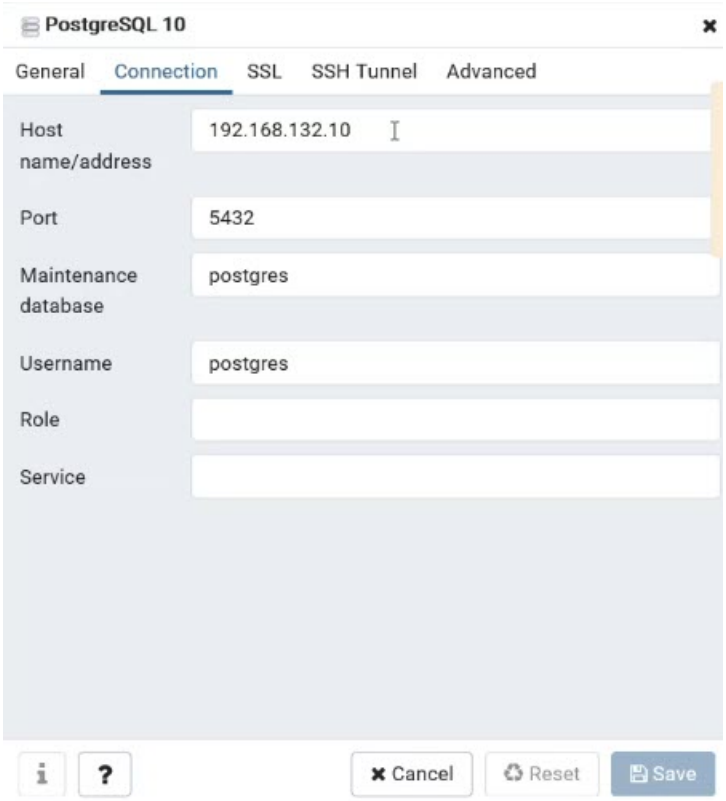
15. Using **PGAdmin**, replace the connection settings for the PG14 server to a disconnected state with values of the PG10 server.

a. Open the **PGAdmin** application.

b. Open the **Servers** drop down menu and right-click **PostgreSQL10**.

c. Click **Properties**. This will open the PostfreSQL10 window, then click **Connection**.

d. Write down the connection settings for PG10.



e. Then navigate to the **Connection** page for **PostgreSQL14** by repeating the above steps.

f. Replace PostgreSQL14's connection settings with the settings copied from PostgreSQL10.

g. Click **Save**.

16. Start the PostgresSQL14 service and check the connection to Pg14 database server with **PGAdmin**.

    a. In the **Services** application, right-click **postgres 14** and click **Start**.

    b. Open **PGAdmin**, click the drop down menu for **Servers** and click **PostgreSQL14**.

    c. Enter the password and click **OK**. A green **Server connected** icon will appear in your screens lower right corner.

17. Go to:

    `https://pas.my.centrify-dev.net`

    Log in to confirm that the migration from PG10/11 to PG14 was successful.

Architectural Overview

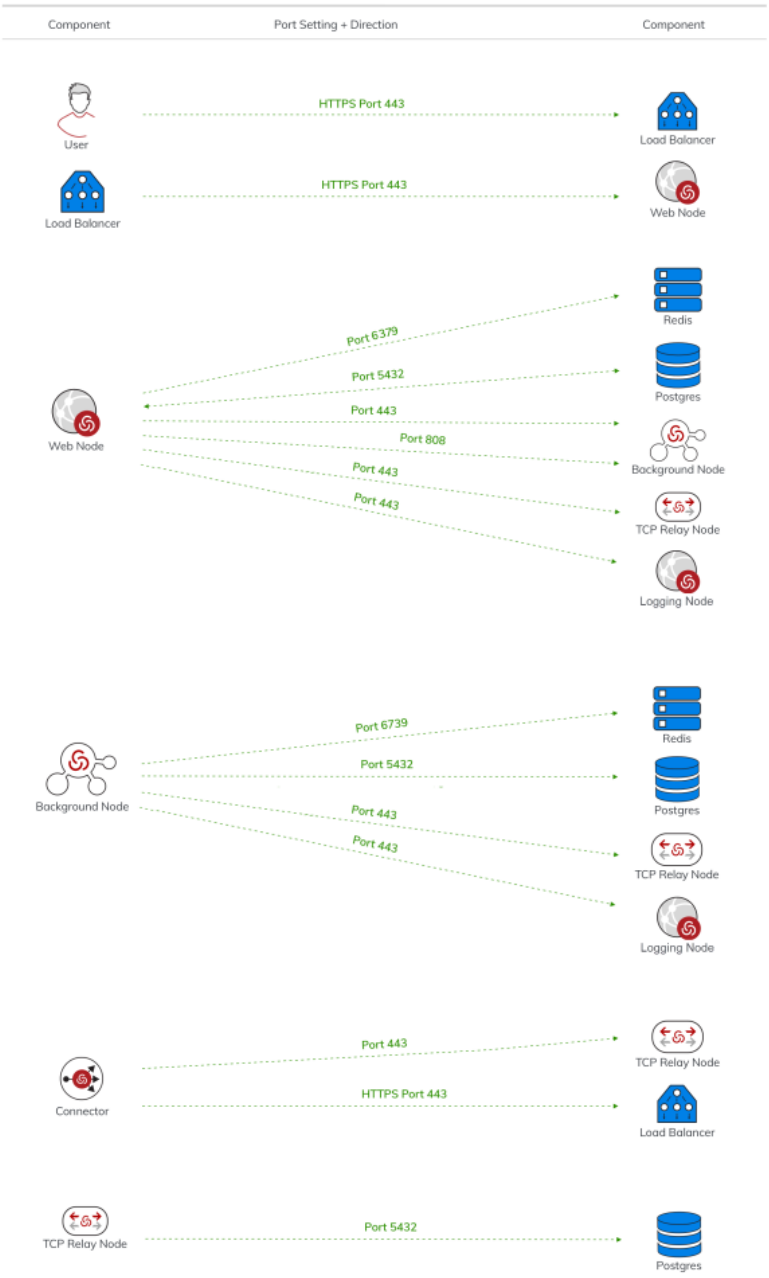
Hyper-scalable PAS utilizes nodes as servers to provide high availability and scale for your infrastructure solution. In Hyper-scalable PAS, when one node fails, the system remains operational (provided you configured with multiple nodes as suggested). The following nodes make up the Hyper-scalable PAS architecture:

- Web node—contains Hyper-scalable PAS software and manages incoming web requests and provides REST endpoints (provides web API functionality). Webnodes communicate with Background nodes, TCP Relay nodes, Cache (Redis), and the Database (PostgreSQL) servers. All user-access to Hyper-scalable PAS is through the Web nodes, which are reached at the host address through the load balancer. The Web nodes do not typically perform long-running or scheduled tasks; their job is to respond quickly to user requests. Only active Web nodes, those with the current active Deployment ID, respond to requests, and therefore only Web nodes receive traffic from the load balancer. You can add more Web nodes to scale up your architecture.
- Background node—contains Hyper-scalable PAS software and manages background jobs such as regularly rotating passwords, re-syncing with the DomainController and running reports. Background nodes communicate with Web nodes, Cache (Redis), and the Database (PostgreSQL) servers. The Jobs dashboard (/jobs) provides a view of the Background node workload. You can add moreBackground nodes to scale up your architecture if you notice delays or jobs are queued for extended periods of time.
- TCP Relay node (Relay and Logging)—Relay and Logging TCP Relay nodes contain Hyper-scalable PAS software and bridge between other technologies such asActive Directory, RDP hosts, log aggregation, and the Hyper-scalable PAS deployment. Although a separate Logging node is not mandatory, Delinea suggests you deploy a separate Logging node.
  - The Relay node allows the Privileged Access Service to communicate with the Connector. Connectors are used to enable Active Directory integration, RDP access, and other integrations with the infrastructure. All TCP Relay nodes receive requests to forward data from Web nodes and/or Background nodes. If a request is Connector-bound (instead of, logging), it is forwarded along the Connector-initiated pipe.
  - The Logging node centralizes the logs onto a single system for easier diagnostics, as well as allowing the logs to be watched on the Management node. The command `Centrify-Pas-WatchLogs.ps1` will not work without a logging node.
- Management node– scripts are executed from the Management node to manage the cluster. The Management node is not part of the cluster itself, however It does need to be able to reach Web, Background and TCP Relay nodes and have full database access. While the management node needs full database access, it doesn't directly communicate with any other nodes beyond the initial installation.

  Note: Each deployed node (Web, Background, and TCP Relay) has an **InstanceID** or **NodeID** that is used to identify that specific server in the Hyper-scalable PAS cluster.
- Database (PostgreSQL) server—external database that is only used for Hyper-scalable PAS. The database (PostgreSQL) never originates requests; it only receives and answers requests.
- Cache (Redis) server—caches repeat operations to improve database performance. The cache (Redis) never originates requests; it only receives and answers requests.
- Load balancer—load balances traffic to multiple servers (for Web node and connector traffic). The load balancer must have a static IP address, with an appropriate entry connecting the name (URI) to the address in the DNS.

Network topology

The following shows the port requirements and direction for Hyper-scalable PAS.



Prerequisites

The following summarizes the minimum software and hardware requirements for deploying Hyper-scalable PAS. Requirements may vary based on your scale out and performance needs; for details see "Scaling and High Availability" on page 190

Database

The database configuration, at a minimum, must have a PostgreSQL-compatible server or cluster with a network reachable service for each Installation. That is, each site (or Installation for a hostname) requires its own database server.

Additional requirements for the PostgreSQL server are noted below:

- PostgreSQL server version 14.9 (or a higher version of 14) or PostgreSQL server version 15, or a managed PostgreSQL service from Amazon Web Service (AWS), Microsoft Azure, or Google Cloud Platform (GCP). Managedservices include: Amazon Relational Database Service (RDS), Amazon Aurora, Azure Database for PostgreSQL, Cloud SQL for PostgreSQL

  Your site specifications for CPU, RAM and disk space are really dependent on workload. However, the server running PostgreSQL at a minimum should include:

  - CPU–a quad-core 2+GHz Intel i7 CPU or equivalent
  - RAM–16GB
  - Disk space–1TB (The amount of disk space in your system is dependent on the amount of data at your site.) Also note that the disk should include priority on disk speed (such as a RAID of SSDs), and RAM (for shared buffer caching) over CPU.
- The following PostgreSQL extensions:
  - postgres_fdw

    postgres_fdw is a foreign data wrapper used to access data stored in remote PostgreSQL servers. See https://github.com/postgres/postgres/tree/master/contrib/postgres_fdw for installation instructions.

The PostgreSQL extensions often come standard if you are using a managed PostgreSQL service.

You can run the following query from a psql prompt to make sure the proper extensions are installed:

Note: If support for older versions of PostgreSQL require the use of the deprecated PLV8 the following query can be executed to validate the PLV8 extension is in use.

```
select * from pg_available_extensions where name in ('plv8','postgres_fdw');
```

- An administrative account with credentials for the database and open port access.

  The username, password, URI and port may be passed to the "Centrify-PAS-NewInstallation" on page 185 command.

  Note: Password authentication supports scram-sha-256 or MD5 for PostgreSQL.
- No Privileged Access Service tables should exist in the database server. If tables do exist, you will need to use the -overwrite flag when issuing the installation command.
- SSL is supported through the `-DBSSL` switch:
  - If PostgreSQL is configured to use SSL, the port specified with DBPort must be the SSL port.
  - If `-DBSSL` is specified, the database server certificate authority chain will be verified, which will fail if the client (the Management, Web, or Background node) does not have all related certificates. `-DBTrustServerSSL` may be used to bypass this check, especially for private authority certificates.

HSPAS Compatibility Matrix

The following table outline the supported PostgreSQL versions for each HSPAS release:

	PG 14	PG 15
RHEL 7.9 EOL June, 3 2024	Not supported	Not supported
RHEL 8.x	Not supported	Not supported
RHEL 8.x w/PLV8	Not supported	Not supported
RHEL 9.2	Not supported	Supported on HSPAS 23.1 HF8
Win 2022	Supported HSPAS 22.3 and 23.1.2	Not supported
Win 2019	Supported HSPAS 22.3 and 23.1.2	Not supported
Win 2016	Supported HSPAS 22.3 and 23.1.2	Not supported

Install the PostgreSQL 15 Database on RHEL 9.2

To install the HSPAS application on a RHEL 9.2 system with a PostgreSQL 15 database, you will need to complete the following steps:

1. Install the RHEL 9.2 operating system on your server.
2. Subscribe your RHEL 9.2 account with a valid account or activation key.
3. Download PostgreSQL 15 using the instructions from the official PostgreSQL download page located here: https://www.postgresql.org/download/linux/redhat/
4. Run the following command to set a password for the PostgreSQL user:

```
[user@localhost ~]$ sudo -u postgres psql
postgres=# ALTER USER postgres PASSWORD '<Enter a password>';
```

5. Open port 5432 to allow remote connections to the PostgreSQL database.
6. Run the following command to install the PostgreSQL 15 library:

```
[user@localhost ~]$ sudo yum install postgresql15-contrib
```

7. Run the following command to check if the 'postgres_fdw' extension is installed:

```
[user@localhost ~]$ sudo find /usr -name postgres_fdw.control
```

8. Run the following commands to enable the 'postgres_fdw' extension in the PostgreSQL database:

```
[user@localhost ~]$ sudo -u postgres psql
postgres=# Run CREATE EXTENSION postgres_fdw;
```

Cache

The caching system, at a minimum, must be a Redis server with a network reachable service for each site and must meet the following requirements:

- At least 2GB of RAM.
- Redis version 4 or above.
- Endpoint is only used for Hyper-scalable PAS.

Refer to the Redis enterprise software overview fore more information on Redis enterprise software.

The following are supported in addition to your hosted Redis service:

- Amazon Web Service (AWS)
- Azure
- Google Cloud Platform (GCP)

Redis is a high-speed cache and is ideally run in a protected network, without passwords or encryption to slow it down. If encrypted communications and protected endpoints are required, both SSL and access key passwords are supported.

The same SSL constraints on PostgreSQL apply to Redis. `-RedisSSL` may be used to require SSL, but then the specified port must be SSL and the server certificate authority chain will be verified. You can use `-RedisTrustServerSSL` if necessary to bypass that.

Note: Web SSH and RDP do not support trust bypass for the Redis certificate.

Redis also supports a password (also known as an “access key”), which may be set using -RedisPassword. Due to command-line constraints, the password may not include quotes, semi-colons, pipes, or other console-impacting special characters.

Load Balancer

A network load balancer (layer 4 – i.e. not a layer 7 or application load balancer) supporting transparent source/target IP and transparent pass-through of SSL (HTTPS) traffic. While Hyper-scalable PAS does transmit via HTTPS, the load balancer must be configured to handle TCP, rather than HTTPS, on port 443; this allows the data encryption to survive the full path between client and server, ensuring security and integrity. Health checks are by HTTPS endpoint.

Load balancers that cannot pass through SSL traffic without decrypting it, such as Amazon's Layer 7 ELB, do not work as they break the full-chain authentication. However, an Amazon Network Load Balancer (ALB) can be configured to pass SSL traffic without decrypting it.

Note: In some cases, load balancers that operate on a different layer or that do not preserve source/target IP, may work, but may impact specific functionality. The load balancer should support dynamically adding and removing servers based on their health check and type.

Certificates for Privileged Access Service Authentication

The primary PAS server in the cluster must contain a certificate that is used for authentication between the PAS and all endpoints that use the PAS (such as enrolled devices, clients, browsers, connector computers, and so on).

The certificate must be for the PAS URI (for example, `vault.mycompany.com`). This is necessary because all endpoints will use the PAS URL host name to access the PAS. All endpoints must trust the certificate authority that issues the host certificate.

When you install the PAS on the primary server in the cluster, you can choose to specify an existing trusted host certificate, or create a new, self-signed certificate. In a production environment, it is recommended that you specify an existing trusted host certificate. The option to create a self-signed certificate during installation is provided mostly for demonstration purposes, and is not intended for use in production environments.

To ensure that endpoints trust the PAS host certificate, the certificate that you specify during installation should be from a known third-party certificate authority (for example, GoDaddy, Verisign, and so on).

During PAS installation on the primary server, you will see the following certificate prompt:

Would you like to provide a custom host certificate, if not, one will be generated for you?

Respond to this prompt in one of these ways:

- To use an existing host certificate from a trusted third-party certificate authority, enter **Y** (yes). You will then be prompted for the location and file name of the certificate.
- To create a new self-signed certificate for demonstration purposes, select **N** (no). A new certificate will be created as part of the installation process.

  Note: If you choose N (no), you will not be able to install the Connector on a separate computer unless the self-signed certificate and root are trusted on the domain.

During PAS installation on secondary servers, you are not prompted for a certificate because certificate information is obtained from a cluster configuration file that is created during primary server installation.

Note: After installation, you can change to a different certificate by executing the `update_host_cert.ps1` script as described in "Updating or Replacing a Web Server Certificate" on page 201.

Supported Redis Versions

Hyper-scalable Privileged Access Service supports Redis versions 4 or greater and has been verified with the following Redis versions:

Redis 4.0.14

Redis 6.0.6

Redis 6.0.10

Note: Ensure your machine meets the minimum requirements for your version of Redis.

License Key

Obtain an Hyper-scalable PAS license key that is specific to your company. During installation, you are required to provide your company name and the license key that is bound to the company name. Contact a Delinea

representative if you do not have a Hyper-scalable PAS license key.

Web, Background, TCP Relay, and Management Nodes

All nodes can be physical, virtual, or cloud instances and must be able to communicate with each other, the database, and the cache (Redis) node. For information on scaling your environment, see "Scaling and High Availability" on page 190. CPU and memory requirements may need to increase as you add users, especially for the Web nodes. The nodes used to run Hyper-scalable PAS must meet the following requirements.

System Requirements

- (General minimum): one Windows Server 2016 or 2019 computer for each node type (Web node, Background node, TCP Relay node, and Management node).
- (HA configuration minimum): at least two Windows Server 2016 or 2019 computers for each node type (Web, Background, and TCP Relay) and oneWindows Server 2016 or 2019 computer for the Management and Logging nodes for a total of 8 computers.
- Computer clock set to synchronize with a known accurate time source.
- Microsoft .NET Framework updated to version 4.8.

  Note: All Hyper-scalable PAS Servers, including the Management node, must have .NET Framework 4.8 installed. As .NET Framework 4.8 is notinstalled on Windows by default, you may have to manually install it. Seehttps://dotnet.microsoft.com/download/dotnet-framework/net48 for information.

- An entry in the Domain Name Server pointing to the load balancer that services the Web nodes.

Additional Management Node Requirements:

The Management node is not required for daily operation.

- Front-end web network accessibility.
- The PKCS #12 SSL certificate file in either .pfx (Personal Information Exchange) or .p12 format (successor format to .pfx) must be available during installation.

connector **computer requirements:**

See the Privileged Access Service *online help* for details regarding "Installing the Connector" on page 189. Ensure you enter the Centrify Privileged Access Service hostname when you register the connectors in your customer-managed Scalable PAS installation.

Network

Make sure your network segment and subnets are defined to allow communication between all nodes within an Installation. For network topology details, see "Architectural Overview" on page 144. Additional network requirements include:

- IP requirements:
  - The load balancer must have an IP address with an appropriate entry connecting the name (URI) to the address in the DNS.
  - The load balancer must be in network mode (layer 4)
- Port requirements
  - Web nodes must be able to accept SSL (port 443) connections from the load balancer node (all calls are SSL).
  - TCP Relay nodes receive connections over port 443, but do not need access to the cache (Redis) or database (PostgreSQL) servers.
- Access to the internet, or–if the computer is not connected to the

  internet–access to installation media for required software. For example,

  IIS, PowerShell, and other features.

Basic Port Requirements

The following table shows the basic port configuration for Hyper-scalable PAS incoming and outgoing component communication. For additional information on port assignments, see "Review the Firewall Rules" on page 6.

Component	Port Setting (Incoming)	Port Setting (Outgoing)
connector	--	443 to various nodes (additionally for AD, RDP, SSH, etc. see "Review the Firewall Rules" on page 6
Load balancer	443	443
Web nodes	443 (from the load balancer)	unrestricted (requires access to Cache Redis and Database PostgreSQL–subnet 443/6379/5432)
Background nodes	443 808	unrestricted (requires access to Cache Redis and Database PostgreSQL–subnet 443/6379/5432)
TCP Relay node	443 (can be limited for IP addresses from the connector and the Web and Background nodes)	443
Redis cache	6379	--
PostgreSQL database	5432	--

PowerShell Execution Policy

The default PowerShell execution policy may prevent the running of unsigned or remote-signed scripts. This will interfere with the execution of Hyper-scalable PAS.The current policy can be displayed with the PowerShell command Get-ExecutionPolicy. It can be set with:

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope CurrentUser
```

Note: Scope could also be `LocalMachine`.

For more information on PowerShell policy, see: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-7.

System Hardening

Things to Know Before You Begin

The following is intended for Windows Server systems only. It assumes you have completed the installation steps as detailed in:

- installed Scalable Privileged Access Service successfully.
- the operating system has been hardened in accordance with either:
  - the Microsoft's Windows Server Security Guide
  - the Center for Internet Security Windows Server (Level 1 benchmarks).

The following should be used in conjunction with any applicable organizational security policies and hardening guidelines. General hardening of the Windows Server instances should be performed before applying the more detailed steps below. If there are conflicts between the following and organizational policy documents, they should be raised with the internal security team for assessment and resolution.

Note: As a general rule, the most restrictive policy that allows for the desired operation of Hyper-scalable PAS without adversely effecting it or any other required element of Windows functionality should be implemented.

All Hyper-scalable PAS components, with the exception of the management node, should be installed on dedicated servers. The servers should not serve any other purpose than that required by the Hyper-scalable PAS solution. The system considered to be direct components of the Hyper-scalable PAS solution are as follows:

- PAS
- Connectors

Windows Operating System Hardening

For Microsoft Windows Server Operating Systems hardening, refer to the Center for Internet Security Level 1 Benchmarks for Windows Server at https://www.cisecurity.org/benchmark/microsoft_windows_server/.

Applying Windows Operating System Updates

Windows updates should be applied in a timely fashion in accordance with the organizational security policy. These may be applied manually or automatically using the Windows Server Update Service (WSUS). Configuration of WSUS is beyond the scope of this document and will also depend on the organization's update strategy. Microsoft provides comprehensive documentation for WSUS and should be consulted as needed.

Using Anti-virus Software

It is recommended consult with your company IT and/or compliance departments to discuss anti-virus needs.

Disabling Network Protocols

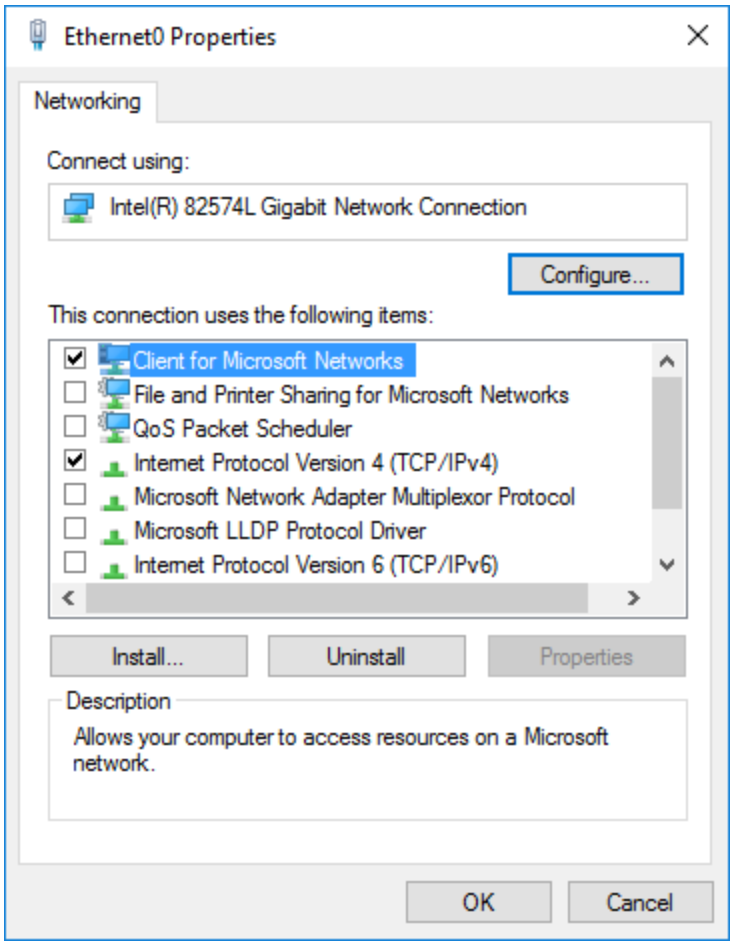
The following networking components are not required by Hyper-scalable PAS or the supporting Windows infrastructure and can therefore be safely disabled on all network adapters:

- File and Printer Sharing for Microsoft Networks.
- QoS Packer Scheduler.
- Microsoft LLDP Protocol Driver.
- Internet Protocol Version 6 (TCP/IPv6).
- Link-Layer Topology Discovery Responder.
- Link-Layer-Topology Discovery Mapper I/O Driver.

This should leave only the following networking components enabled:

- Internet Protocol Version 4 (TCP/IPv4).
- Client for Microsoft Networks.

The following image illustrates how the network adapter properties should look following these changes:



Network Adaptor Properties

Configuring Windows Logging and Auditing

By default, Windows Server does not log all events of potential interest. Unless organizational policies mandate them and they have previously been enabled, perform the following steps:

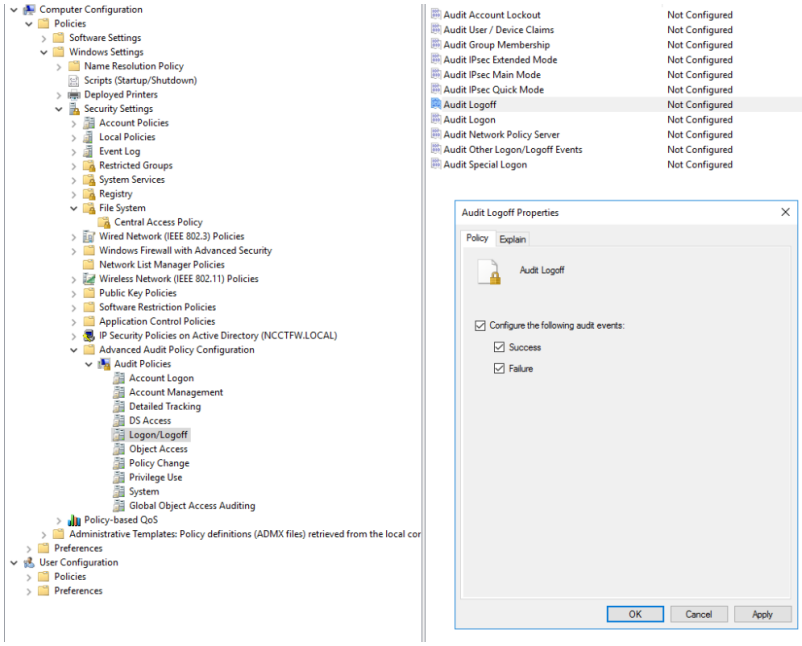
1. Go to Start Menu > Administrative Tools > Group Policy Management. In the left pane, navigate to Forest > Domains > Domain Name. Expand it.
2. If it does not already exist, create a new Group Policy Object called “Delinea”by right-clicking on Domain Name and selecting Create a GPO in this domain and link it here....
3. Right-click on the “Delinea”policy object.
4. Click Edit in the context menu. It shows Group Policy Management Editor. Navigate to Computer Configuration > Policies → Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies. It lists all audit policies in the

right pane. Here, enable the following policies for both “Successful” and “Failed” events:

5. Configure the following keys as follows:

Key	Value
Logon/Logoff → Audit Logoff	Success & Failure
Logon/Logoff → Audit Logon	Success & Failure
Object Access → Audit Detailed File Share	Success & Failure
Object Access → Audit File Share	Success & Failure
Object Access → Audit File System	Success & Failure
Object Access → Audit Registry	Success & Failure
Object Access → Audit Handle Manipulation	Success & Failure

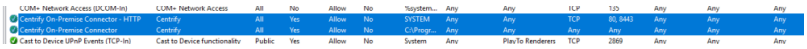
After making the above changes open an Administrative command prompt and enter gpupdate/force.



Audit Logoff

Verifying Firewall Configuration

During the installation process, the Windows Firewall is correctly configured to allow Hyper-scalable PAS components to operate correctly. No further steps should be required. If a firewall other than the Windows Firewall is in use, it must be configured according to the following values:



Disabling Default Accounts

Disabling Default Accounts

The local administrator account should be disabled to prevent its use. Before you do this, ensure you have another administrative account configured.

To disable local administrator account, enter the following command into an administrative command prompt:

net user administrator /active:no

The same steps should be taken for the "Guest" and "DefaultAccount" accounts.

To list the accounts present on a server, enter the following command into an administrative command prompt:

net users

To learn if a given account is active or not, enter the following command into an administrative command prompt:

net user <account name>

For instance, net user guest should return output of the following form:

Note: Note the line "Account active No."

C:\Windowssystem32\>net user guest

User name Guest

Full Name

Comment Built-in account for guest access to the computer/domain

User's comment

Country code 000 (System Default)

Account active No

Account expires Never

Password last set 14/09/2018 15:41:54

Password expires Never

Password changeable 14/09/2018 15:41:54

Password required No

User may change password No

Workstations allowed All

Logon script

User profile

Home directory

Last logon Never

Logon hours allowed All

Local Group Memberships *Guests

Global Group memberships *None

The command completed successfully.

Disabling Unnecessary Default Shares in Windows

To disable the share, perform the following steps:

Disable default shares on all Hyper-scalable PAS servers by running regedit (Windows key + R → regedit) and setting the value of the following registry key to (REG_DWORD) 0:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters AutoShareServer

Create the AutoShareServer key if it does not already exist .

Restart the server.

To confirm the change run the following in a command prompt: net share

The result should be as follows:

C:\>net share

Share name Resource Remark

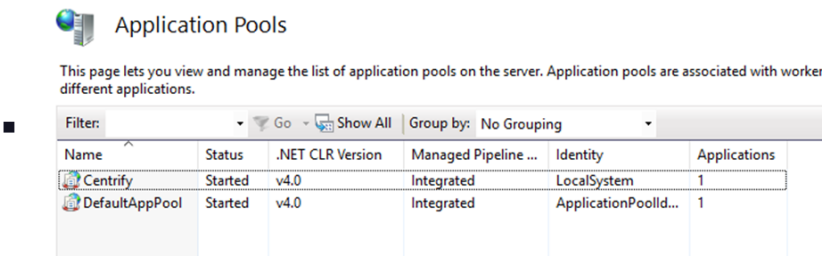
IPC$ Remote IPC

The command completed successfully.

Windows Internet Information Server (IIS) Hardening

Perform the following steps:

1. Remove all unnecessary IIS Application Pools on all Hyper-scalable PAS servers.
2. Start Internet Information Services (IIS) Manager (Windows Key + R → inetmgr).
3. Open the Application Pools leaf under the server being managed and remove all application pools apart from the DefaultAppPool and the Delinea entry. The results should appear as follows:



4. Restart the server.

Securing Hyper-scalable PAS

Understanding Hyper-scalable PAS User Password Policy

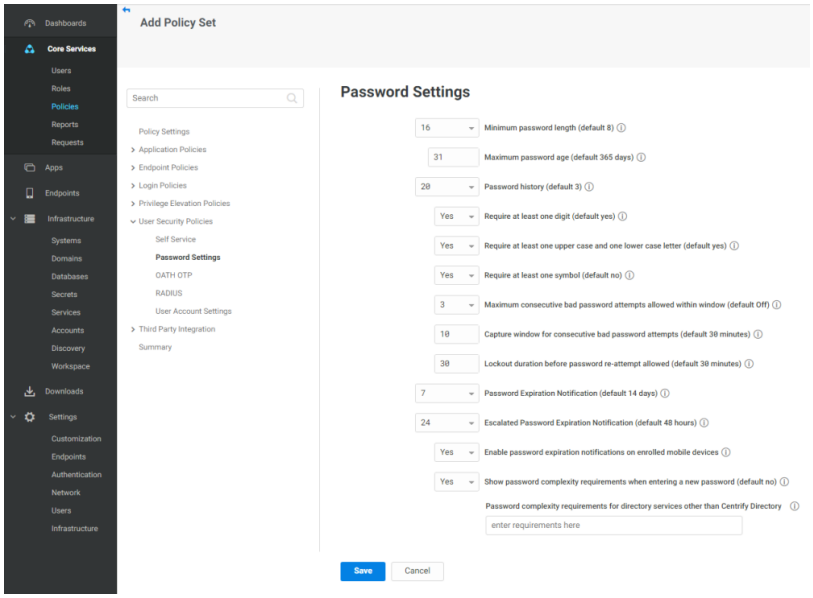
Due to the sensitivity of the information and functionality handled by a Hyper-scalable PAS implementation, the standard organizational password policies might not provide adequate protection. The following settings are recommended for Hyper-scalable PAS users.

1. To apply these polices, log into the Admin Portal and navigate to Core Services → Policies → Add Policy Set.
2. Under User Security Policies → Password Settings set the values above as follows:

Setting	Recommendation
Minimum password length	16 characters
Maximum password age	31 days
Password history	20

Setting	Recommendation
Require at least one digit	yes
Require at least one upper case and one lower case letter	yes
Require at least one symbol	yes
Maximum consecutive bad password attempts allowed within window	3
Capture window for consecutive bad password attempts	10
Lockout duration before password re-attempt allowed	30
Password expiration notification	7
Escalated password expiration notification	24
Enable password expiration notification on enrolled devices	yes
Show password complexity requirements when entering a new password	yes

Alternatively, if there is an available OAUTH or RADIUS solution in place, with appropriate password policies, these may be configured in the same place.

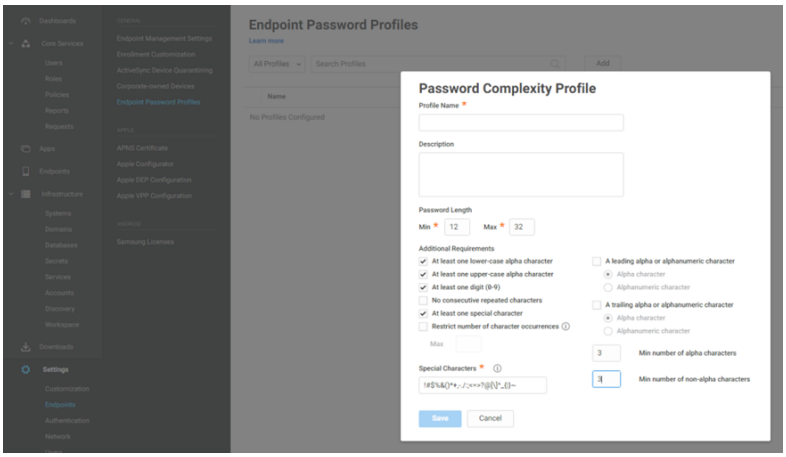


Password Profiles

Endpoint and Infrastructure Password Profiles

The following password policy settings are recommended to enforce a strong level of protection for endpoints and infrastructure using Hyper-scalable PAS.

1. To apply these policies, log into the Admin Portal and navigate to Settings → Users > Password Profiles → Add.



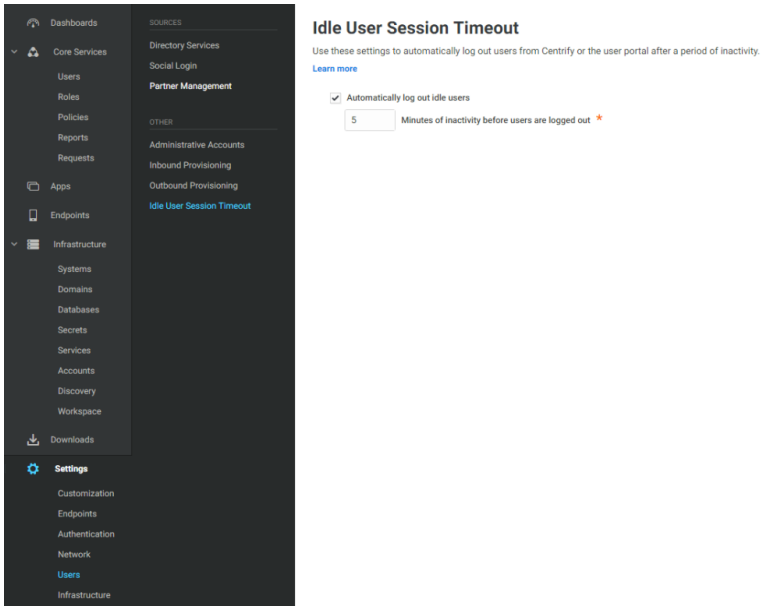
2. Create new profiles with the following values:

Setting	Recommendation
Minimum password length	12
Maximum password length	32 (or greater)
At least one lower-case alpha character	Checked
At least one upper-case alpha character	Checked
At least one digit	Checked
No consecutive repeated characters	Checked
At least one special character	Checked
Restrict number of character occurrences	Checked (3)
Special characters	!#$%&()*+,-./:;<=>?@[\]\^_{|}~
A leading alpha or alphanumeric character	Unchecked
A trailing alpha or alphanumeric character	Unchecked
Min number of alpha characters	3
Min number of non-alpha characters	3

Setting Idle User Timeout

Users should be timed out and required to re-authenticate after a period of inactivity exceeding five minutes. This setting can be configured through the Admin portal by:

1. Navigating to Settings → Users → Idle User Session Timeout.
2. Automatically Logout Idle Users should be checked and a value of 5 entered for the Minutes of inactivity before idle users are logged out setting.



- Idle User Session Timeout

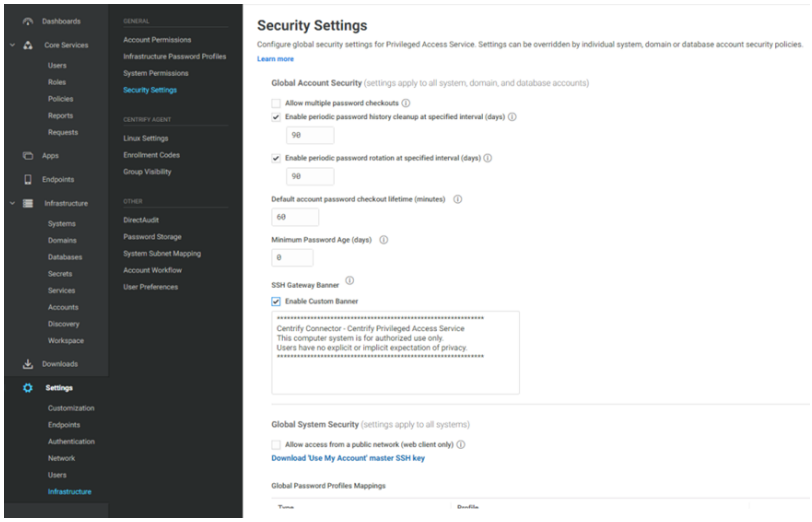
Reviewing Infrastructure Security Settings

To enforce a strong level of protection for endpoints and infrastructure using Hyper-scalable PAS the following settings password policy settings are recommended:

Setting	Recommendation
Allow multiple password checkouts	Unchecked
Enable periodic password history clean-up at specified interval	Check and set to 90
Enable periodic password rotation at specified interval	Check and set to 90
Default account password checkout lifetime	60

Setting	Recommendation
Minimum password age	0
SSH Custom Banner	Checked and set according to organizational security policy

To apply these policies, log into the Admin Portal and navigate to Settings → Authentication → SecuritySettings.



Windows Server Update Services (WSUS)

Microsoft pushes updates and reboots to your systems. For this reason, it is strongly recommended you follow the best practice of running a Windows Server Update Services (WSUS) for your installation cluster. This allows you control of the updates. Configure as follows:

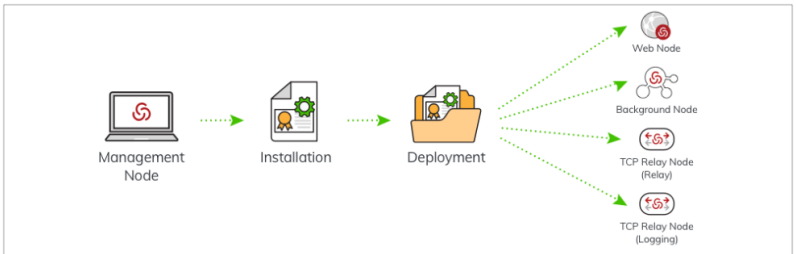
- Configure WSUS to only install upon administrator approval.
- Automatic updates must be disabled.
- Deploy new nodes with the latest operating system patches and with the current deployment package. Then, decommission the nodes in need of an operating system update.

For more information on WSUS, see Windows Server Update Services (WSUS).

Installing Hyper-scalable PAS

As a solution that you manage, the Hyper-scalable PAS replicates the infrastructure provided by the Privileged Access Service using your own servers. The installation procedures described in this section install the necessary software on Windows Servers to configure them for the following:

- Management node
- Web node
- Background node
- TCP Relay node (for relay)
- TCP Relay node (for logging)



You may choose from two installation scenarios:

- Minimum installation suitable for evaluation only
- Multiple server installation suitable for production

Minimum Installation for Evaluation Only

Before you Install

Before you install the Delinea Hyper-scalable PAS software, ensure you have the following (refer to "Prerequisites" on page 146 for details).

- A license key
- (Optional) Host certificate from a trusted certificate authority, issued for the hostname that you will access Hyper-scalable PAS through. For evaluation purposes, you can use an automatically generated certificate.

  Note: Wildcard certificates can be used.

- Windows server for your configuration
- (Optional) Redis server
- (Optional) PostgreSQL-compatible database with all required extensions installed. If you do not have a suitable database to use, one can be installed for you as part of the installation process.
- Data connection information for the following:
  - **Redis:** server hostname, server port (default is 6379), SSL
  - (Optional) **Database:** user name, password, server hostname, server port (default is 5432). This is only required if your existing setup uses a database.
  - **Hostname:** this is the name of the Installation and must match the hostname used on the certificate
- (Required for some services) Connector.

Note: Not all services require a Connector. See the Privileged Access Service *online help* and see "Installing the Connector" on page 189 to determine if your configuration requires a connector.

Multiple Server Installation Suitable for Production

The scripts provided for installation have embedded help, which you can view using the Get-Help command; for example, from the script directory type, `Get-Help .\Centrify-PAS-NewDeployment.ps1`. More detailed help about the parameters is available using the `-detail` flag. For example, `Get-Help .\Centrify-PAS-NewDeployment.ps1 -detail`. Additional command output, useful for debugging or watching progress, is available using the `-verbose` switch.

Note: All examples in this section, use pas.corpnet.com to refer to the Hyper-scalable PAS hostname.

Before you Install

Before you install the CentrifyHyper-scalable PAS software, ensure you have the following:

- A license key
- Host certificate from a trusted certificate authority issued for the hostname that you will access Hyper-scalable PAS through.

  Note: Wildcard certificates can be used. <
- Windows server for your configuration "Prerequisites" on page 146 for this bullet and the three that follow)
- Redis server
- Load balancer
- PostgreSQL-compatible database with all required extensions installed
- Data connection information for the following:
  - **Redis:** server hostname, server port (default is 6379), SSL
  - **Database:** user name, password, server hostname, server port (default is 5432).
  - **Hostname:** this is the name of the Installation and must match the hostname used on the certificate
- Computer designated for the Connector, if applicable. (Not all services require a Connector.) See the Privileged Access Service*online help* and see "Installing the Connector" on page 189 to determine if your configuration requires a connector.

Installing Using the Installer PowerShell Script

The following is an overview of the steps, organized into phases, required to install Hyper-scalable Privileged Access Service. Detailed procedures of each phase are described in subsequent sections.

Phase 1: Installing the Management Node

- Download / copy the Hyper-scalable PAS zip package from Delinea to the Windows server you have designated to be the Management node.

You will need the following software components from the zip package:

- `install.ps1`
- `CentrifyPlatform-[Build.Number].zip`

- Create the Management Node

  To create the Management node, open an elevated PowerShell session and run the install.ps1 script. This expands and installs the`CentrifyPlatform-[Build.Number].zip`. Once completed, the necessary scripts are available on the Management node for installation and deployment.

  The command can receive an optional target parameter, which indicates where to install the deployment. The default value is `C:\centrify`.

  Change to the target directory (`C:\centrify` or as specified on the install command line) for all subsequent Management node commands.

Phase 2: Creating a new Installation

- Create a new installation using the `Centrify-PAS-NewInstallation.ps1` command

  on the Management node. This will do the following:

  - Creates the configuration file
  - Verifies the configuration inputs
  - Checks for the Redis and database servers
  - Initializes the database
  - Checks for the required database extensions

Phase 3: Creating a Deployment Package

- Create your deployment package using the `Centrify-PAS-NewDeployment.ps1` command on the Management node.

  You can enter a unique Deployment ID using the `-ID` parameter; otherwise a GUID is used as the Deployment ID.

Phase 4: Deploying Hyper-scalable PAS software to Web, Background, and TCP Relay Nodes

- Copy the Deployment Package from the `installations\<hostname>\Deployments` subdirectory, to target systems.Once copied, uncompress the package and run the extracted`Centrify-PAS-Deploy.ps1` command with the node type as the parameter for each node installation. For example:

  ```
  .\Centrify-PAS-Deploy.ps1 -BackgroundNode
  ```

  The command can receive the `InstallPath` parameter, which indicates where to install the deployment. The default value is `C:\CentrifyNode`.

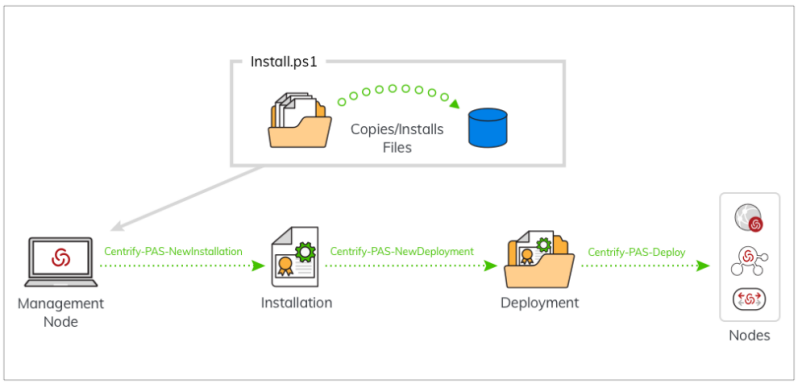
  Install the logging node first, if applicable, and then at least one Web node, Background node and TCP Relay node per site installation.

Phase 5: Activating the Deployment

- From the Management node, activate the deployment using the `Centrify-PAS-SetActiveDeployment.ps1` command.
- Pass in the Deployment ID that you either set as a parameter or received as output from the `Centrify-PAS-NewDeployment.ps1` script.
- From the Management node, you can run the command `Centrify-PAS-NodeList`before activating the deployment, to verify the installation and to ensure the nodes are recognized. This should show all of the deployed nodes with an Inactive status. If you run `Centrify-PAS-NodeList` again (after activating your deployment), you should see that the Web and Background node status is now Active.

> **Note:** The scripts provided for this installation support the PowerShell switch`-verbose` which enables you to view additional data about the command.

Phase 1: Installing the Management Node



To install the Hyper-scalable PAS, the first step is to create the Management node. Download the Hyper-scalable PAS software package to the computer designated as the Management node and then run the Hyper-scalable PAS installer (`install.ps1`). The software package contains a directory structure with the following items:

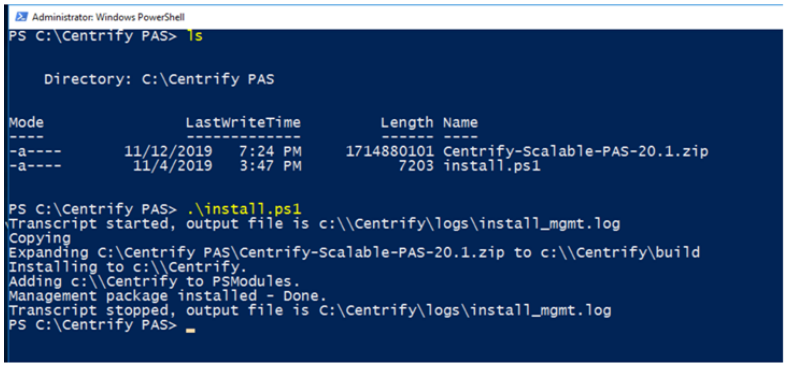
- Documentation (PDF)
- CentrifyPlatform-[Build.Number].zip (contains the Hyper-scalable PAS installation package)
- `install.ps1` (expands and installs the `CentrifyPlatform-[Build.Number].zip` file)

To Install the Management Node

1. On the Management node, log in as a user with administrator rights.
2. Download the Hyper-scalable PAS software package from Delinea onto the Management node.
3. Open a PowerShell session in elevated (`RunAs Administrator`) mode.

> **Note:** All PowerShell sessions must be elevated; that is `RunAs Administrator` mode.

4. If the installer package is a single zip file, expand it (`Expand-Archive` in PowerShell, or your preferred unzipping tool).
5. At the PowerShell prompt, type `.\install.ps1` to set up PowerShell cmdlets and tooling on the Management node for cluster installation, management, and deployments.



See the additional parameters below.

Parameter	Description
[-target <String>]	Type in the location for the installation (for example, C:\ Centripas; if the target is not included the default is C:\centrify).

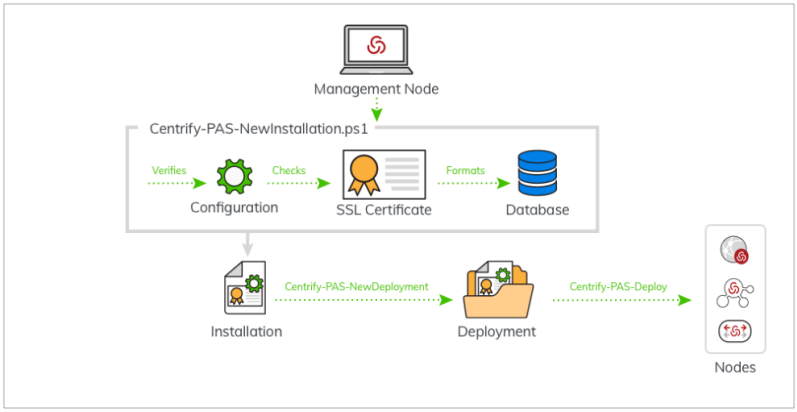
Type `Get-help .\install.ps1 -detail` to get information on parameters and switches.

1. Once installed the following scripts are available in the specified target

   directory:

   - `Centrify-PAS-ForceRemoveNode.ps1`
   - `Centrify-PAS-GetDeployment.ps1`
   - `Centrify-PAS-ModifyInstallation.ps1`
   - `Centrify-PAS-NewDeployment.ps1`
   - `Centrify-PAS-NewInstallation.ps1`
   - `Centrify-PAS-NodeList.ps1`
   - `Centrify-PAS-SetActiveDeployment.ps1`
   - `Centrify-PAS-WatchLogs.ps1`

Phase 2: Creating a New Installation



After creating the Management node, use the Centrify-PAS-NewInstallation.ps1 script, available on the Management node, to create a new Installation. An Installation is an instance of a cluster (all resources, nodes, configuration information, that together provide a single cluster), operating with a single hostname (for example, pas.corpnet.com). The number of systems that comprise the cluster depends on your environment (for minimum requirements, see "Prerequisites" on page 146.

Creating a new Installation requires a dedicated database; this is specified in the configuration or parameters. Each installation must have its own database on a dedicated PostgreSQL server.

The `Centrify-PAS-NewInstallation.ps1` script

- Creates a directory to hold the generated installation data (in `<Centrify PAS Directory>\installations`).
- Creates a configuration in a config subdirectory (inside the installations directory for this installation). The command parameters are passed as individual parameters or configured in a prepared file.
- Verifies the configuration inputs (makes sure the hostname resolves to the DNS, checks for the database and Redis servers, that the database credentials work, and that the proper database extensions are installed).
- Verifies that the database does not have a current installation; if it does, the installation fails. To override this, either delete the database or use the `-override` switch (note you cannot recover your data after using the override switch).
- Initializes the database (this destroys any data in the database).
- Accepts the installation license key.

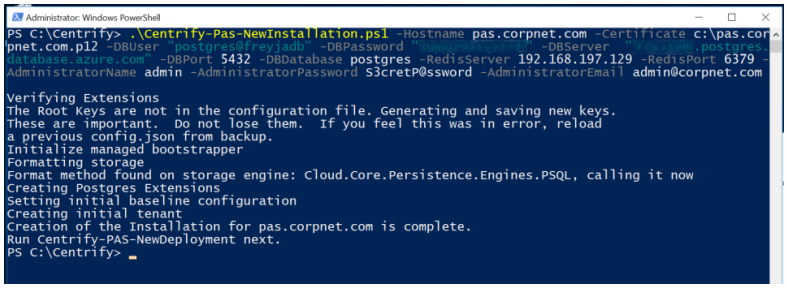
To Create a New Installation

1. If you are not already logged in to the Management node, log in as a user with administrator rights.
2. At an elevated PowerShell prompt, run `.\Centrify-PAS-NewInstallation.ps1.`

   The script options can be provided on the command line. For example:

   ```
   .\Centrify-PAS-NewInstallation.ps1
   -Hostname pas.corpnet.com  -Certificate C:\corpnet.com.p12  -DBUser centrifyAccount  -
  DBPassword secretCode  -DBServer postgres.corpnet  -RedisServer cache.corpnet -
  AdministratorName PASAdmin -AdministratorPassword EvenMOreS3cret  -AdministratorEmail
  pasadmin@corpnet.com   -CompanyName Corpnet  -LicenseKey 234KL43
   ```

   Type `Get-help .\Centrify-PAS-NewInstallation.ps1 -detail` to get information on the command and parameters, or see "Centrify-PAS-NewInstallation" on page 185.

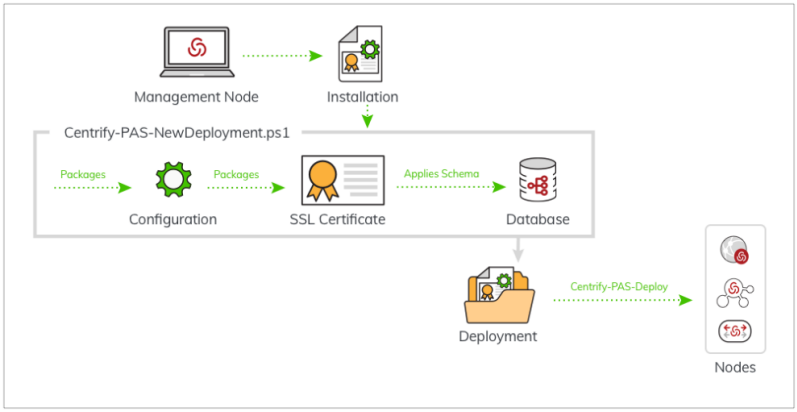
   

   Note: You can also pass configuration parameters via config.json file. If you use this method, you need to populate the config.json file with the required data prior to running the script, see "Configuration File" on page 174.

   If the command is successful, a zip file is created and available in the installations directory (`\Installations\Config\<hostname>.zip`) on the Management node.
3. Copy the newly-created configuration directory to a safe and secure location.

   Note: The configuration directory contains the generated certificates and keys for your installation, so it is important that you do not lose the contents.

Phase 3: Creating a Deployment Package



Once an Installation is defined, use the `Centrify-PAS-NewDeployment.ps1` to create a Deployment package (a .zip file) that you can distribute to cluster nodes (Web nodes, Background nodes, and TCP Relay nodes). The `Centrify-PAS-NewDeployment.ps1` script updates the database schema and creates a Deployment in a new folder under the `Installations<hostname>\Deployments` directory on the Management node, with the current date and the Deployment ID (as specified or as a GUID). Inside that directory is a single file called `<Deployment ID>.zip` that includes everything needed to create Web, Background, and TCP Relay nodes, including the configuration and certificate data.

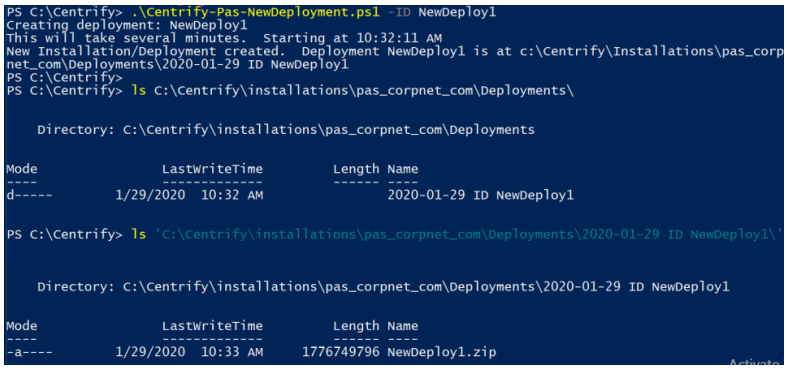
Note: An Installation must be created (see *Phase 2: Creating a New Installation* above prior to running the deployment package script.

To Create a Deployment Package

1. If you are not already logged in to the Management node, log in as a user with administrator rights.
2. Change to the target directory and at the PowerShell prompt, type `Centrify-PAS-NewDeployment.ps1 [-Hostname][[-ID]]`. See the following example:

   ```
   .\Centrify-PAS-NewDeployment.ps1 -Hostname pas.corpnet.com -ID NewDeploy1
   ```

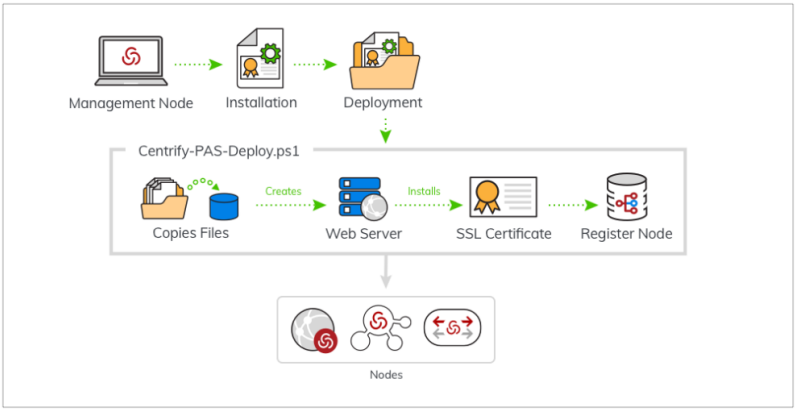
   Type `Get-help .\Centrify-PAS-NewDeployment.ps1 -detail` to get information on the command and parameters or see "Centrality-PAS-NewDeployment" on page 184.



3. Once complete the following file is available in the `...\installations\<hostname>\Deployments\<date-DeploymentID>\` directory:

   `<deployment_id>.zip`

Phase 4: Deploying Hyper-scalable PAS Software to Web, Background, and TCP Relay Nodes



After you complete the steps in previous sections, you copy the Deployment file (`<deployment_id>.zip`) from the Management node to each target node (Web, Background, TCP Relay) and then run `Centrify-PAS-Deploy.ps1` to build each node. The illustration above depicts the deployment process. The deployment process is the same for each node with the exception of the command node type parameter.

When deploying (via `Centrify-PAS-Deploy.ps1`) a new Deployment, in addition to Web and Background nodes, you can also deploy two types of TCP Relay nodes: Logging node and the regular Relay node.

Note: Delinea strongly recommends you install the Logging node first (if applicable), allowing the Web and Background nodes to see and log in to it.

To Install Each Node

You need to perform these procedures for each node (Web, Background, TCP Relay, and Logging node) in the Installation.

1. Copy the deployment file, `<deployment_id>.zip`, from the Management node to the target node (the Windows servers designated as a Web, Background, TCP Relay, or Logging nodes).

   The `<deployment_id>.zip` file is created in `\installations\<hostname>\Deployments\<date-DeploymentID>\` when you create the deployment package. See "To Create a Deployment Package" on the previous page.

2. On the target node, unzip the `<deployment id>.zip` file using the Expand-Archive commandlet or your preferred utility.

3. On the target node, run the `Centrify-PAS-Deploy.ps1` script with the appropriate parameter for the desired node type (see "Centrify-PAS-Deploy" on page 180 for a list of parameters).

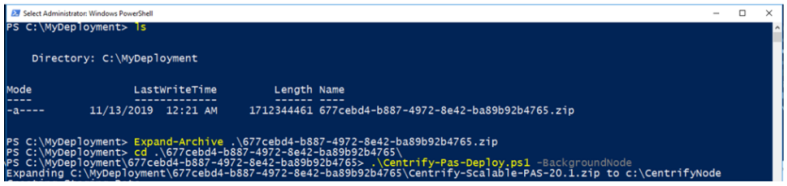
   Delinea strongly recommends you install the Logging node first (if applicable), to allow the Web and Background nodes to see and log in to it.

The command can receive the InstallPath parameter, which indicates where to install the deployment. The default value is `C:\CentrifyNode`.

For example, to create a Background node you enter:

```
.\Centrify-PAS-Deploy.ps1 -BackgroundNode
```

Type `Get-help .\Centrify-PAS-Deploy.ps1 -detail` to get information on the command and parameters, or see "Centrify-PAS-Deploy" on page 180.



Phase 5: Activating the Deployment

There are two steps to activating a new Deployment. From the Management node:

- Ensure that the load balancer can send traffic to the Web nodes.

  Note that Web nodes fail the health check until they are set to active.
- Activate new nodes (Web and Background) by switching to the new Deployment ID.

When the Web node deployment is completed, add the new Web nodes to the target list of your load balancer. The health check URI is `/health/check`. Verify that the hostname resolves to the load balancer on your DNS, and then you are ready to activate the deployment so that it can service requests.

Note: The Background nodes should have the same Deployment ID, but the load balancer only points at Web nodes.

When creating a new deployment, a new Deployment ID is created or assigned. Once the deployment is created, new nodes can be created, but those nodes won't respond to traffic until the load balancer points to the new Web nodes, and the new Deployment is set to Active. To activate inactive nodes, you run the `.\Centrify-PAS-SetActiveDeployment.ps1` script from the Management node, specifying the desired Deployment ID.

At this point, any nodes in a previous Deployment ID are inactive and show as unhealthy or down in your load balancer, while the new nodes with matching Deployment IDs are active and show as healthy or up. Depending on the load balancer settings there may be a delay.

Note: Hyper-scalable PAS does not support deactivating and then reactivating a deployment directly. Whenever a node is deactivated via `Centrify-PAS-SetActiveDeployment`, it must be rebooted before reactivating it.

To Activate the Deployment

1. From the Management node, type the following to set the Deployment to active:

   ```
   Centrify-PAS-SetActiveDeployment.ps1 [-Hostname] <String> [-ID] <String>
   ```

Type `Get-help .\Centrify-PAS-SetActiveDeployment.ps1 -detail` to get information on the command and parameters or see Centrify-PAS-SetActiveDeployment.

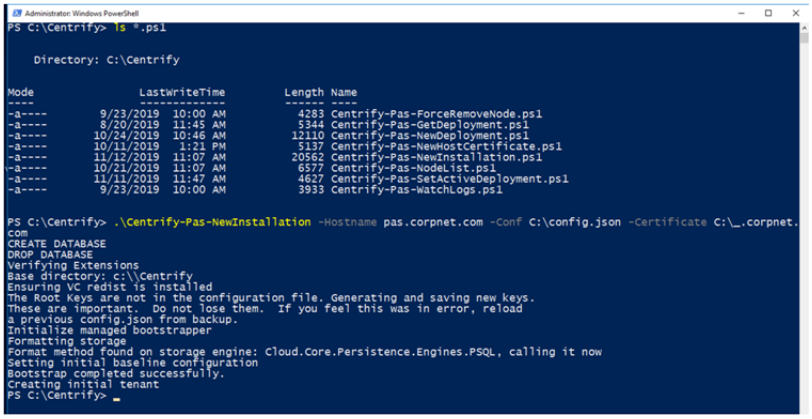
2. Once the installation is complete, you can start using the Privileged Access Service.

Configuration File

During installation and deployment of Hyper-scalable PAS, you populate a configuration file with installation details using a JSON formatted file (`config.json`). The `Centrify-PAS-NewInstallation.ps1`requires this information during installation (see *Phase 2: Creating a New Installation* above.

To automate the process, you can add the information to `config.json` file yourself. Using this method, you enter the data directly into the `config.json` file prior to running the `Centrify-PAS-NewInstallation.ps1` script. The file is stored in the `installations\Config\hostname` subdirectory. Ensure you back up the configuration directory to a safe and secure location, as this has the generated certificates and keys for your installation.

The following is an example of using the `config.json` to pass parameters in the `Centrify-PAS-NewInstallation.ps1` script.



You must provide the following information for the config.json file:

- Redis: server hostname, server port (default is 6379)
- Database: user name, password, server hostname, server port (default is 5432)
- Hostname: this is the name of the installation and must match the hostname used on the certificate

Sample config.json File

Contents of config.json file:	Description
{	
"Redis": {	
"ServerHost": "myredis",	ServerHost: Enter hostname or an IP address.
"ServerPort": "6379",	
"UseSSL": "False"	
},	
"Database": {	
"UserName": "dbuser",	UserName: Often defaults to postgres.
"Password": "secretPassword",	
"ServerHost": "postgres.mycorp.net",	ServerHost: Name or IP Address of server.
"ServerPort": "5432"	
},	
"Hostname": "pas.corpnet.com",	Hostname: Must match the host certificate or be in its wildcard.
"Administrator": {	
"UserName": "admin",	UserName: Enter an administrator login name. It should not match an Active Domain account user name.
"Password": "tellNobody",	Password: Password for the Centrify admin account.
"Email": "admin@corpnet.com",	Email: Enter the email account information for the admin account.
},	
}	
}	

To Update Log locations Using config.json

Note: Default log locations are already set, therefore you only need change the config.json if you want to change the default log locations.

Before running Create-Pas-NewDeployment, update the logging section. For example:

```
"Logging":  {
    "CloudFolder":"C:\\CentrifyLogs\\Cloud",
    "LintFolder":"C:\\CentrifyLogs\\Lint",
    "AnalyticsFolder":"C:\\CentrifyLogs\\Analytics",
    "RelayFolder":"C:\\CentrifyLogs\\Relay"
}
```

Hyper-scalable PAS Sizing Guidelines

The Hyper-scalable PAS platform has many features and use-cases. This page provides a baseline guide to use as a starting point.

Note: Larger or smaller setups can be extrapolated from this guide.

The following key use cases have been tested and observed.

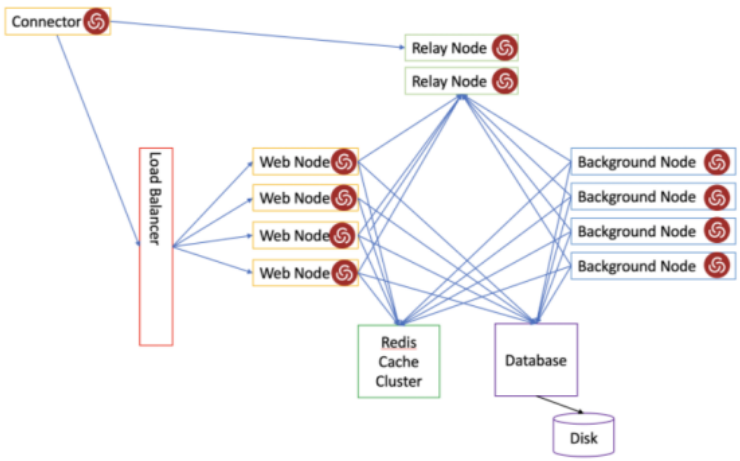
Note: Testing is an ongoing process and specifications may need to be adjusted on a case-by-case basis.

Use case	Description
Cloud Agent	- Back-channel traffic impact on TCPRelay, web, and background nodes
	- Password management / reconciliation traffic
PAS	- RDP web and native session traffic
	- SSH web and native session traffic
	- Password management / reconciliation traffic

On-premise Example

Below is a configuration for an on-premise Hyper-scalable PAS using VMware vSphere consisting of the following machines:

Name	Specifications	Server
2x Connector node 4 core	16GB RAM	Windows Server 2016
2x TCPRelay nodes 4 core	16GB RAM	Windows Server 2016
2x Worker nodes 4 core	16GB RAM	Windows Server 2016
3x Web nodes 4 core	16GB RAM	Windows Server 2016
Logger node 2 core	16GB RAM	Windows Server 2016
Management node 2 core	8GB RAM	Windows Server 2016
PostgreSQL DB 8 core	32GB RAM	Centos 7, PostgreSQL 10.14 single node
Redis cache 8 core	32GB RAM	Centos 7, Redis 6.0.8-1 single node



Capabilities

This configuration is capable of the following concurrent sessions:

- 50 (medium traffic) RDP web sessions

  Note: Traffic was simulated by running the task manager which generates RDP traffic via periodic screen updates.

- 350 (low-medium traffic) SSH sessions

  Note: Traffic was simulated by running top, which generates SSH traffic via periodical screen updates.

- 1000 - 1500 Cloud Agents (depending on activity)

  Note: Traffic was simulated using an internal tool.

When using this example as a basis, keep in mind:

- All of these numbers can be serviced via a single connector but we recommend having more than one for redundancy.
- *(Optional)* Connectors may be configured to provide only specific services to isolate traffic / load.
- *(Optional)* TCPRelays may also be configured to provide a dedicated BackChannel communications for Cloud Agent.
- This example does not generate any consequential load on:

  - PostgreSQL database
  - Redis load. Latency was measured to be:
    - Minimum: 0 ms
    - Maximum: 1 ms (spiked up to 2-3 ms during agent enroll)
    - Average: .05 ms
- Resource impact. See Load impact section below for use-case specifics.

Load Impact

The primary load on a Hyper-scalable PAS system is on the web nodes and primarily affects the CPU and RAM resources. This is due to external communications which require the web nodes, such as:

- Web browser UI
- REST
- Agents
- Data requiring backend (worker node)

The second critical component are the connectors. All web and direct session access without the Portal is directed through the connector machine. This load is primarily seen as total network traffic throughput and the number of concurrently open network sockets.

Note: The TCPRelay load is seen as total network traffic throughput and the number of concurrently open network sockets. The CPU and RAM utilization will be very low.

There is no significant load on PostgreSQL or Redis.

Comparable Environments

Below is a comparable Amazon EC2 instance: Other machine requirements can be extrapolated from these baselines.

Name	AWS EC2 instance	vSphere
Management node	t2.large	2 core 8 GB RAM
Logger node	t3.xlarge	4 core 16 GB RAM
PostgreSQL	db.r4.2xlarge	8 core 32 GB RAM
Redis	cache.r4.large	No direct comparison but you can use the PostgreSQL instance as a baseline.
TCPRelay nodes	t3.xlarge	4 core 16 GB RAM

Name	AWS EC2 instance	vSphere
Web nodes	t3.xlarge	4 core 16 GB RAM
Worker nodes	t3.xlarge	4 core 16 GB RAM
Connector nodes	t3.xlarge	4 core 16 GB RAM

Note: The information in a sample setup only. You may require sizing adjustments based on your specific setup.

Cloud Agent

Cloud Agent generates a negligible load on Hyper-scalable PAS from login and MFA operations. The Cloud Agent has a back-channel communication path with Hyper-scalable PAS that enables Delinea to provide features such as:

- Agent-assisted account reconciliation
- Workflow
- On demand provisioning
- HealthCheck

Note: This back-channel does not require customers to open additional ports. It provides a mechanism for various Platform components to invoke remote functionality on the Clients.

The Cloud Agent will register itself via the back-channel by default during the enrollment process or agent start-up.

Note: The default settings are configurable.

Once the Cloud agent registration is complete, back-channel traffic may be generated for the following reasons:

- Periodic HealthCheck (configurable) every hour per agent
- `cinfo -H` will perform a HealthCheck
- Feature management capability
- Password reconciliation capability

On shutdown, the Cloud Agent unregisters itself from the back-channel.

These operations do not inherently constitute a large amount of traffic or load. However, when multiplied by a large number of enrolled Cloud Agents, this can present occasional spikes in the back-channel traffic, which can affect performance.

For example, the following may create a large spike in BackChannel registration traffic:

- An automated / orchestrated provisioning of a large number of machine instances within a short period of time
- Auto-enrolling Cloud Agents.

Note: TCPRelays can be configured to be dedicated for Cloud Agent use only.

Privileged Access Service

RDP and SSH access via a web browser is a key feature of Hyper-scalable PAS. This system was able to support:

- 50 RDP web sessions
- 350+ SSH web sessions

Hyper-scalable PAS Command Reference

The scripts / commands described in this section are used to install and manage the Hyper-scalable PAS. These commands are available once you download the Hyper-scalable PAS software package to the computer designated to be the Management node. Once the software package is downloaded, you run the Hyper-scalable PAS installer (install.ps1) to install the software package which contains a directory structure with the following items:

All PowerShell sessions must be elevated; that is RunAs Administrator mode.

Centrify-PAS-Deploy

Once the Deployment file (<deployment_id>.zip) is copied from the Management node to a target node (Web, Background, TCP Relay) and unzipped (e.g., using Expand-Archive), running Centrify-PAS-Deploy.ps1 installs and creates the node. The deployment process is the same for each node with the exception of the command node type parameter.

In addition to Web and Background nodes, you can also deploy two types of TCP Relay nodes: Logging node and the regular Relay node.

Usage:

.\Centrify-PAS-Deploy.ps1 [-BackgroundNode] [-RemoveNode] [-Report] [-ID] <String> [-URI] <String>

Example:

.\Centrify-PAS-Deploy.ps1 -BackgroundNode -ID PrimaryBackground

Command parameters:

Parameter	Description
[-WebNode] [-BackgroundNode] [-RelayNode] [-LoggingNode] [-RemoveNode]	Enter the node type where you are deploying the software. String variance depends on node type. Remove this node from the cluster. (Decommission.)

Parameter	Description
[-Report]	Provides data for the installed node.
[-ID]	(Optional ID) Enter a unique instance ID to act as a node identifier. If you do not enter a value, a GUID is created. The ID must be unique across the installation, but is not verified at deployment, so only use this parameter if you're certain it is unique.
[-URI]	(TCP Relay or Logging nodes only) Hostname or IP Address that can reach the TCP Relay or Logging Service. If not provided, the internal network address is used.

Centrify-PAS-ForceRemoveNode

Use Centrify-PAS-ForceRemoveNode.ps1 to remove an unused or malfunctioning node from the Hyper-scalable PAS installation. This does not decommission the node on the server. Generally, you should run the Centrify-PAS-Deploy -RemoveNode command on the node to be removed.

Usage:

.\Centrify-PAS-ForceRemoveNode.ps1 [-Hostname] <String> [-Node] <String>

Example:

.\Centrify-PAS-ForceRemoveNode -Hostname pas.corpnet.com -Node PrimaryBackgroundNode

Command parameters:

Parameter	Description
[-Hostname]	Enter the hostname you use to define the Installation (for example, pas.corpnet.com). This also serves as the configuration name in the Installations\Config directory. The Hostname defines the Installation.
[-Node]	Enter the name of the node you want to remove (for example. WebNode, BackgroundNode, RelayNode, or LoggingNode)

Centrify-PAS-GetDeployment

Use the Centrify-PAS-GetDeployment.ps1 command to see if a deployment is active. Running this command from the Management node retrieves the currently-active Deployment ID for all the nodes associated with the installation.

Usage:

.\Centrify-PAS-GetDeployment.ps1 [-ListDeployments]

Command parameters:

Parameter	Description
[-ListDeployments]	Enter the Deployment ID to get a list of nodes associated with the installation.

Centrify-PAS-ModifyInstallation

Use the Centrify-PAS-ModifyInstallation.ps1 command to modify an existing Hyper-scalable PAS Installation. You can change significant elements of the installation, such as:

- Changing the PostgreSQL database or database credentials
- Changing the Redis (cache) server
- Rotating the TCP Relay node certificates
- Changing the host certificate

In order to implement the changes, you must create and deploy a new deployment to Web and Background nodes.

Usage:

.\Centrify-PAS-ModifyInstallation.ps1 [[-Hostname] <String>] [[-NewHostname] <String>] [[-Certificate] <String>] [[-CertificatePassword] <String>] [[-DBUser] <String>] [[-DBPassword] <String>] [[-DBServer] <String>] [[-DBPort] <String>] [[-DBDatabase] <String>] [[-RedisServer] <String>] [[-RedisPort] <String>] [[-RedisPassword] <String>] [-DBSSL] [-DBTrustServerSSL] [-NewRelayCertificate] [-NewLoggingRelayCertificate] [-DBNoPLV8] [-RedisSSL] [<CommonParameters>] (Deprecated)

Note: The RedisTrustServerSSL parameter is not supported in Web RDP/SSH.

Example:

.\Centrify-PAS-ModifyInstallation.ps1 -Hostname pas.corpnet.com -Certificate c:_corpnet.p12

Command Parameters:

Parameter	Description
[-Hostname]	Enter the hostname you use to define the Installation (for example, pas.corpnet.com). This also serves as the configuration name in the Installations\Config directory. The Hostname defines the Installation.
[-NewHostname]	(Optional) Replacement hostname for the installation. If set, the installation files will be moved to a new matching directory, and the previous Installation will be marked "Deprecated". Note: Use this with caution.

Parameter	Description
[-Certificate]	Enter the source location for the new certificate, if not specified in the configuration file. Make sure that the certificate used is from a trusted certificate authority, is PKCS #12 SSL in either .pfx (Personal Information Exchange) or .p12 format (successor format to .pfx), and the hostname is supported by the certificate. Hyper-scalable PAS does not generate self-signed certs.
[-CertificatePassword]]	(Optional) Passphrase for the supplied certificate. If provided, the passphrase used to extract the plain text certificate, which is stored in the configuration.
[-DBUser]	Type the user name used to log in to the database, if not specified in the configuration file.
[-DBPassword]	Type the password credential used to log in to the PostgreSQL database, if not specified in configuration file.
[-DBServer]	Enter the server hostname (URI) for PostgreSQL, if not specified in configuration file.
[-DBPort]	Enter the PostgreSQL server port, typically 5432, if not specified in configuration file.
[-DBDatabase]	Enter the PostgreSQL database name to use when verifying access, if not specified in configuration file.
[-RedisServer]	Enter the Redis server hostname (URI), if not specified in configuration file.
[-RedisPort]	Enter the Redis server port, typically 6379, if not specified in configuration file.
[-RedisPassword]	Enter the Redis access key if required.
[-DBSSL]	Specifies to use SSL to communicate to the database.
[-DBTrustServerSSL]	Tells the client to accept the server without verifying the certificate chain. See SSL information in the Prerequisites section for more detail.
[-NewRelayCertificate]	Use this parameter to generate and configure a new security certificate for the TCP Relay node. Note: This is only necessary when your certificates have been compromised. Once you run this command, any previous TCP Relay nodes will stop working, since their security parameters do not match. You must create a new deployment and deploy new TCP Relay nodes.

Parameter	Description
[NewLoggingRelayCertificate]	Use this parameter to generate and configure a new security certificate for the TCP Relay Logging node. This is only necessary when your certificates have been compromised. Once you run this command , logging to the TCP Relay Logging node stops working as the security parameters do not match. You must create a new deployment and deploy a new TCP Relay Logging node, then restart Web and Background nodes.
[-DBNoPLV8] (Deprecated)	Required if this switch was previously used, to bypass checking the database for PLV8.
[-RedisSSL]	Specifies that SSL (TLS 1.2 or 1.3) is to be used with Redis.
	This cmdlet supports the common parameters: Verbose, Debug,ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, PipelineVariable, and OutVariable. For more information, see about_CommonParameters.
[-RedisTrustServerSSL]	This parameter is not supported in Web RDP/SSH.

Centrality-PAS-NewDeployment

The Centrify-PAS-NewDeployment.ps1 creates a Deployment package (a .zip file) that you can distribute to cluster node machines (Web nodes, Background nodes, and TCP Relay nodes). The Centrify-PAS-NewDeployment.ps1 script updates the database schema and creates a Deployment in a new folder under the Installations\<hostname>\Deployments directory on the Management node, with the current date and the Deployment ID (as specified or as a GUID).

Usage:

.\Centrify-PAS-NewDeployment.ps1 [-Hostname] <String> [-ID] <String>

Example:

.\Centrify-PAS-NewDeployment.ps1 -Hostname pas.corpnet.com

Command parameters:

Parameter	Description
[-Hostname] <String>	Enter the hostname you use to define the Installation (for example, pas.corpnet.com). This also serves as the configuration name in the Installations\Config directory. The Hostname defines the Installation.
[-ID] <String>	(Optional) Enter a unique ID (such as First, Second, Third) to set the new Deployment ID. The Deployment ID acts as the Installation version to identify the Deployment and to determine which nodes are active and inactive. You can see it when you issue the NodeList command. If you do not provide an ID, a GUID is created and used to identify the Installation version. Only alpha-numeric characters are allowed.

Centrify-PAS-NewInstallation

The first step in creating a new installation is to run the Centrify-PAS-NewInstallation.ps1 command on the Management node. This creates the configuration file, verifies the configuration inputs, checks for the Redis and database servers, initializes the database, and checks for the required database extensions.

You can also pass configuration parameters via config.json file. If you use this method, you need to populate the config.json file with the required data prior to running the script.

Note: Do not re-run Centrify-PAS-NewInstallation.ps1 on a configuration with active data, as it will reformat the database and destroy the data. Use Centrify-PAS-ModifyInstallation instead.

Usage:

.\Centrify-PAS-NewInstallation.ps1
[-Hostname] <String>
[-Certificate]<String>
[-DBUser] <String>
[-DBPassword] <String>
[-DBServer] <String>
[-RedisServer] <String>
[-AdministratorName] <String>
[-AdministratorPassword] <String>
[-AdministratorEmail] <String>
[-CompanyName] <String>

Example:

.\Centrify-PAS-NewInstallation.ps1
-Hostname pas.corpnet.com
-Certificate C:\corpnet.com.p12
-DBUser centrifyAccount
-DBPassword secretCode
-DBServer postgres.corpnet
-RedisServer cache.corpnet
-AdministratorName PASAdmin
-AdministratorPassword EvenM0reS3cret
-AdministratorEmail pasadmin@corpnet.com
-CompanyName Corpnet
-LicenseKey 234KL43

Command parameters:

Parameter	Description
[-Hostname] <String>	Enter the hostname you use to define the Installation (for example, pas.corpnet.com). This also serves as the configuration name in the Installations\Config directory. The Hostname defines the Installation.
[-Conf] <String>	Enter the source location for the configuration file (config.json) to copy values from. This is updated and stored in the installations\Config\hostname subdirectory, for use by Centrify-PAS-NewDeployment.ps1.
[-Certificate] <String>	Enter the source location for the certificate. Make sure that the certificate used is from a trusted certificate authority, is PKCS #12 SSL in either .pfx (Personal Information Exchange) or .p12 format (successor format to .pfx), and the hostname is supported by the certificate. Hyper-scalable PAS does not generate self-signed certs.
[-DBDatabase] <String>	Enter the PostgreSQL database name to use when verifying access, if not specified in configuration file.
[-DBServer] <String>	Enter the server hostname (URI) for PostgreSQL, if not specified in configuration file.
[-DBPort] <String>	Enter the PostgreSQL server port, typically 5432, if not specified in configuration file.
[-DBUser] <String>	Type the user name used to log in to the database, if not specified in the configuration file.
[-DBPassword] <String>	Type the password credential used to log in to the PostgreSQL database, if not specified in configuration file.
[-DBSSL]	Specifies to use SSL to communicate to the database.
[-DBTrustServerSSL]	Tells the client to accept the server without verifying the certificate chain. See SSL information in the Prerequisites section for more detail.
[-RedisServer] <String>	Enter the Redis server hostname (URI), if not specified in configuration file.
[-RedisPort] <String>	Enter the Redis server port, typically 6379, if not specified in configuration file.
[-RedisPassword] <String>	Enter the Redis access key if required.
[-RedisSSL]	Specifies that SSL (TLS 1.2 or 1.3) is to be used with Redis.

Parameter	Description
[-AdministratorName] <String>	Enter the name for initial administrative account, if not specified in configuration file.
[-AdministratorPassword] <String>	Enter the password for initial administrative account, if not specified in the configuration file.
[-AdministratorEmail] <String>	Enter the email address for initial administrative account, if not specified in the configuration file.
[-CompanyName] <String>	Enter the company name exactly as it appears in the license key data.
[-LicenseKey] <String>	Enter the license key for this installation. The license key is provided by Delinea.

Centrify-PAS-NodeList

This command provides a lists of all nodes (Web, Background, and Relay) associated with the Hyper-scalable PAS installation and their status. The following status information is available:

- Active: a status of Active indicates that the node is part of the current deployment.
- Inactive: a status of Inactive indicates that the node is registered with a different Deployment ID than the current active one.
- Online: indicates a node is running and connected to the database.
- Offline: indicates a node that is not running or not able to connect to the database.

Note: Even though TCP Relay nodes have an associated Deployment ID, they are not tied to a Deployment. For a TCP Relay node, the Deployment ID is considered to be the version rather than a grouping, as they don't parse or handle data structures.

Usage:

.\Centrify-Pas-NodeList.ps1 [-Hostname] <String>] [-Detailed] [-Relays] [-DiagnosticRelays]

Example:

```
PS C:\centrify> .\Centrify-Pas-NodeList.ps1 -table

Node Type          Instance ID    IP Address   Online? Active? Deployment
---------          -----------    ----------   ------- ------- ----------
Web                Web.192.122    10.0.192.122 Online  Active  Ver.20.2
Background         Worker.192.124 10.0.192.124 Online  Active  Ver.20.2
TCPDiagnosticRelay Logger.192.129 10.0.192.129         N/A     Ver.20.2


PS C:\centrify>
PS C:\centrify> .\Centrify-Pas-NodeList.ps1


Host        : pas.corpnet.com
Node Type   : Web
Instance ID : Web.192.122
IP Address  : 10.0.192.122
Online?     : Online
Active?     : Active
Deployment  : Ver.20.2

Host        : pas.corpnet.com
Node Type   : Background
Instance ID : Worker.192.124
IP Address  : 10.0.192.124
Online?     : Online
Active?     : Active
Deployment  : Ver.20.2

Host        : pas.corpnet.com
Node Type   : TCPDiagnosticRelay
Instance ID : Logger.192.129
IP Address  : 10.0.192.129
Online?     :
Active?     : N/A
Deployment  : Ver.20.2

PS C:\centrify>
```

Command parameters:

Parameter	Description
[-Hostname] <String>	Enter the hostname used for the deployment you want to access. This command impacts all hostnames (of which there should really be just one), but allows for partitioning of the configurations.
[-Detailed] <SwitchParameter>]	List out the system info (CPU, Disk, etc.) for each node at the time of Deployment. Does not apply to TCP Relay nodes or Relay Logging nodes.
[-Relays] <SwitchParameter>	Displays active TCP Relay data.
[-DiagnosticRelays] <SwitchParameter>	Displays active Logging data.

Centrify-PAS-SetActiveDeployment

Use the Centrify-PAS-SetActiveDeployment.ps1 command to switch to the new Deployment ID and activate new nodes (Web and Background). The Deployment ID is created or assigned when creating a new deployment. Once the deployment is created, new nodes can be created, but those nodes won't respond to traffic until the load balancer points to the new Web nodes, and the new Deployment is set to Active. To activate inactive nodes, you run the .\Centrify-PAS-SetActiveDeployment.ps1 script from the Management node, specifying the desired Deployment ID.

Any nodes in a previous Deployment ID are inactive and show as unhealthy or down in your load balancer, while the new nodes with matching Deployment IDs are active and show as healthy or up. Depending on the load balancer settings there may be a delay.

Usage:

.\Centrify-PAS-SetActiveDeployment.ps1 [-Hostname] <String> [-ID] <String>

Example:

.\Centrify-PAS-SetActiveDeployment -Hostname pas.corpnet.com -ID Aug21Deploy

Command parameters:

Parameter	Description
[-Hostname] <String>	Enter the hostname used for this deployment. This command impacts all hostnames (of which there should really be just one), but allows for partitioning of the configurations.
[-ID] <String>	Enter the Deployment ID or GUID to activate the deployment.

Centrify-PAS-WatchLogs

Use the Centrify-PAS-WatchLogs.ps1 command to watch or capture logs from the Web, Background, and Relay nodes. The command Centrify-Pas-WatchLogs.ps1 does not work without a dedicated logging node.

Usage:

.\Centrify-Pas-WatchLogs.ps1 [-Hostname] <String>]

Example:

.\Centrify-Pas-WatchLogs.ps1 -Hostname pas.corpnet.com

Command parameters:

Parameter	Description
[-Hostname] <String>	Enter the hostname you use to define the Installation (for example, pas.corpnet.com).

Installing the Connector

To install the Connector for a Hyper-scalable PAS instance, refer to the documentation for "How to Install a Connector" on page 409 but with the following stipulations:

Note: Before you install the Connector, you must first install the TCP Relay node. For information on how to install the TCP Relay node, see "Installing Hyper-scalable PAS" on page 163.

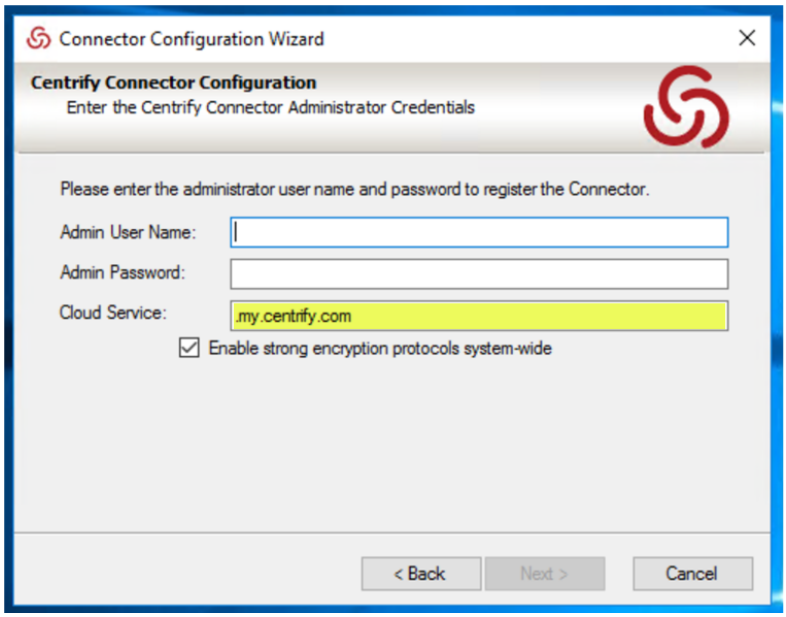
1. Download the Connector installer:
   a. Log in to the host computer with an account that has sufficient Connector permissions to install the connector.
   b. Open the Admin Portal.

c. In the navigation pane, click **Downloads** and search for "Connector" or scroll down to see the connector file.

d. Next to the Connector file, click **Download** to download a zip file.

e. Extract the zip file and then run the installer program **Centrify-Connector-Installer-<version>.exe**.

2. Run the downloaded package, which launches the Connector Configuration Wizard.



Scaling and High Availability

Hyper-scalable PAS resources are easily scaled up to provide more processing capability while also providing a highly available environment. As the volume of processing expands, adding additional Web and Background nodes distribute the workload, allowing traffic to be spread out over multiple nodes. Additionally, in the event of a system failure on one of the nodes, the additional nodes in the configuration are available to provide uninterrupted service as the failed node is replaced.

To ensure that your data is always available and that your environment can withstand system failures while optimizing system performance, follow the suggestions in this section.

Scale Your Environment to Balance Your Workload

As the load on your Hyper-scalable PAS installation increases, you may notice slower authentication and Admin Portal responses, or that the time to generate reports and synchronization has increased.

To handle incoming authentication requests and slower Admin Portal responses, you can add more Web nodes to your Installation. To add additional systems, see the following procedures:

- "Phase 3: Creating a Deployment Package" on page 166
- "Phase 4: Deploying Hyper-scalable PAS software to Web, Background, and TCP Relay Nodes" on page 166
- "Phase 5: Activating the Deployment" on page 167

You can use ASP.Net Performance Counters to monitor performance of:

- Current connections
- Requests in application queue
- Processor – % processor time
- Memory – available Mbytes

See https://stackify.com/asp-net-performance-counters/ for information on using ASP.Net.

To evaluate Background node load, look for a line such as the following:

```
2020-04-12 18:34:38,955 [DevInstance-DevInstance|1d65a33bcaba4f4db97b2e1bfd5038a3|275|(null)|(null)|566070|INFO |(null)] JobMonitor:
CloudFire Metrics: 0 jobs in Queue, plus 1 jobs running.
Average Queue Time: 0; Longest: 0
Longest Running Job: 203997 for Job ID: ABC0123:f729408a-fa46-f373-0c00-2a94a51e6f29, Tenant: ABC0123
```

In general, you should expect very few jobs to be queued as jobs should be in the running state quickly. If jobs are queued but no jobs are running, you may need to restart the Background nodes. If jobs are running and yet there are multiple queued jobs, adding another Background node allows more jobs to run simultaneously, clearing out the queue.

Provide Uninterrupted Service in the Event of System Failure (High Availability)

Use the "Centrify-PAS-WatchLogs" on page 189 command to monitor your environment and watch or capture logs from the Web, and Background nodes. If you detect an error in one of the Web or Background nodes, and your configuration contains more than one Web or Background node, you can easily replace the faulty system without interrupting the service. To avoid a single point of failure in your Hyper-scalable PAS solution, be sure that the other components, such as cache, database, Connector, load balancer are also scaled up.

Note that node monitoring is dependent on your organizations chosen software. For information on replacing a faulty system and disaster recovery, see the following sections:

- "Backup and Disaster Recovery" on page 208
- "Changing to a New Redis (cache) Server" on page 207
- "Changing to a New Database Server or Updating Database Connection Properties" on page 206

Updating Hyper-scalable PAS Software

This section describes how to update the Hyper-scalable PAS release to a new version of the software, where the Privileged Access Service is already installed and running. To prevent downtime while updating the software, you create new nodes and deploy the new software to those nodes. Once the new nodes are deployed, you then add the new Web nodes to the load balancer, and change to the new deployment, setting the new nodes to active.

For example, if your configuration includes three Web nodes, two Background nodes, and two TCP Relay nodes deployed as Deployment A, you would deploy three new Web nodes, two new Background nodes, and two TCP Relay nodes as Deployment B. Once the new nodes are deployed, you add the Deployment B Web nodes to the load balancer (listener target) server group, which now includes six Web nodes. Since Deployment B is not active yet, no traffic is sent to the Deployment B Web nodes. Once Deployment B is set to active, traffic into the load balancer is sent to the Deployment B Web nodes and the nodes in Deployment A become inactive.

Updating Hyper-scalable PAS involves the following main tasks:

- Download the updated Hyper-scalable PAS software package, see "Phase 1: Installing the Management Node" on page 167
- Update the database schema and create an updated Deployment on the Management node, see "Phase 3: Creating a Deployment Package" on page 171.
- Copy the new deployment file to new Windows Server to create new nodes, see "Phase 4: Deploying Hyper-scalable PAS Software to Web, Background, and TCP Relay Nodes" on page 172
- Add the new Web nodes to the load balancer and activate the deployment, see "Phase 5: Activating the Deployment" on page 173
- After the load balancer shows the new nodes as healthy and distributing traffic, remove the nodes from the previous deployment. You can then tear down or reformat the nodes from the previous deployment.

To Update Hyper-scalable PAS on the Web, Background, and TCP Relay Nodes

The following step-by-step instructions augment the update overview provided above.

1. On the Management node, log in as an user with administrator rights.
2. See "Phase 1: Installing the Management Node" on page 167 to download and unzip the updated Hyper-scalable PAS software package from Delinea onto the Management node.

   Note: Do not run `Centrify-PAS-NewInstallation.ps1` on an existing installation; **doing so destroys all the current data.** After creating an initial Installation, the Installation is updated using the `Centrify-PAS-NewDeploy.ps1`; **not** using `Centrify-PAS-NewInstallation.ps1` again.

3. See "Phase 3: Creating a Deployment Package" on page 171 file in the `...\installations\<hostname>\Deployments\<date-DeploymentID>\` directory.
4. See "Phase 4: Deploying Hyper-scalable PAS Software to Web, Background, and TCP Relay Nodes" on page 172 TCP Relay Nodes to copy the updated deployment file,`<deployment_id>.zip`, from the Management node to the new target nodes.
5. See "Phase 5: Activating the Deployment" on page 173 to add the Web nodes to the target list of your load balancer and set nodes to active.
6. From the nodes you want to remove, type `Centrify-PAS-Deploy-RemoveNode` command.

You can then tear down or reformat the nodes from the previous deployment.

Configuring a Web Server Certificate for PAS

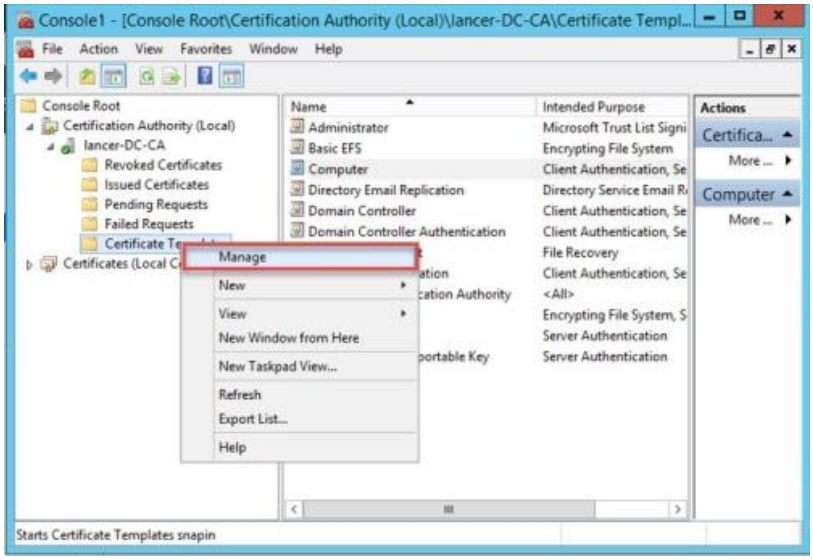
To create a web server certificate for your Delinea PAS environment, perform the following steps:

1. Create a web server certificate template with an exportable private key.
2. Generate a wildcard certificate for your web servers (*.domain.com).
3. Export the certificate plus the private key into a file.

To Create a Web Server Certificate Template with an Exportable Private Key

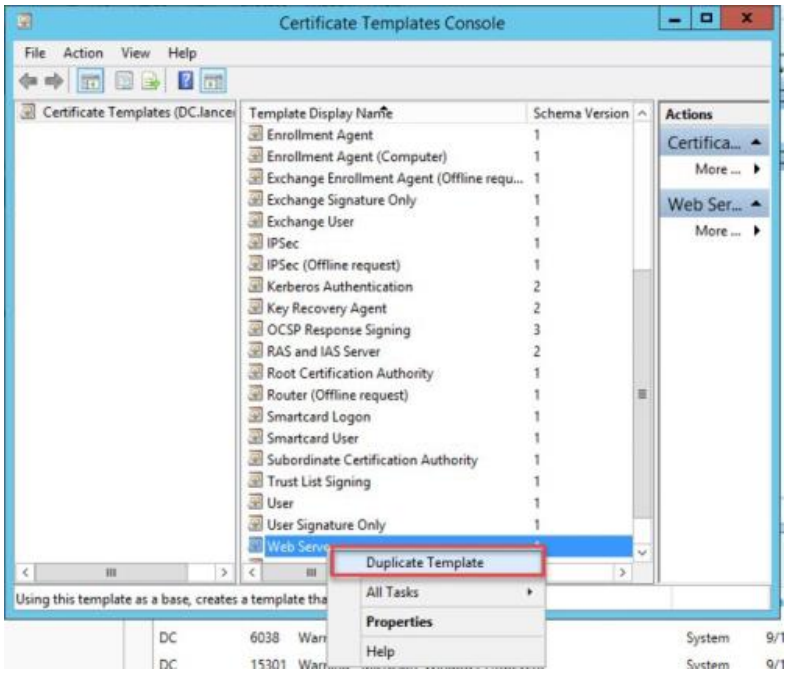
To create a web server certificate template to allow exporting for private keys, perform the following steps:

1. In your domain's Certification Authority (CA), open the Certification Authority program and expand the CA.
2. Right-click Certificate Templates and select Manage. This opens the Certificate Templates console.



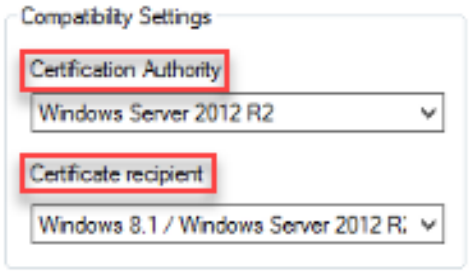
- Manage Certificate Templates

3. Scroll down and right click the Web Server template and select Duplicate Template This opens the new certificate template window.

- 

- Duplicate Template

4. Navigate to the Compatibility Settings tab:
   a. For the Certification Authority field, select Windows Server 2012 R2 or higher.
   b. For the Certificate Recipient fields, select Windows 8.1/ Windows Server 2012 R2 or higher.

- 

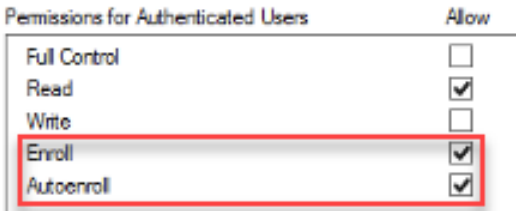
- Certificate Authority and Recipient

5. Navigate to the General tab > Template display name and set it to “Web Server with Exportable Key” (no quotes).
6. Navigate to the Request Handling tab and check the checkbox “Allow the private key to be exported.”

- 

- Allow Private Key Export

7. Navigate to the Security tab. Here, authenticated users are highlighted. In the lower pane, check the boxes for Enroll and AutoEnroll.

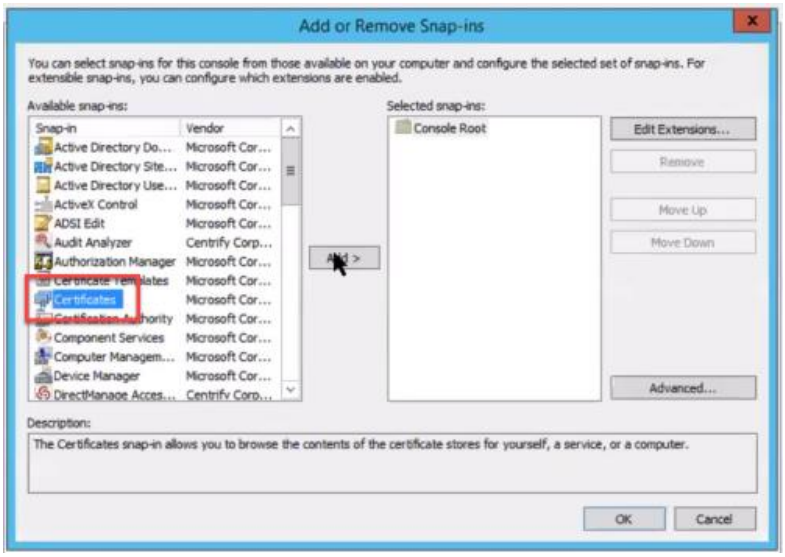


- Enroll and AutoEnroll

8. Click OK. This will save this new Certificate Template and close the Certificate Templates Window.
9. Back in the Certification Authority console, right click Certificate Templates > New > Certificate Templates to Issue. This opens the Enable Certificate Templates window.
10. Scroll down to Web Server with Exportable Key and click OK. The modified template is now ready for use through group policy.
11. Close the Certification Authority console.

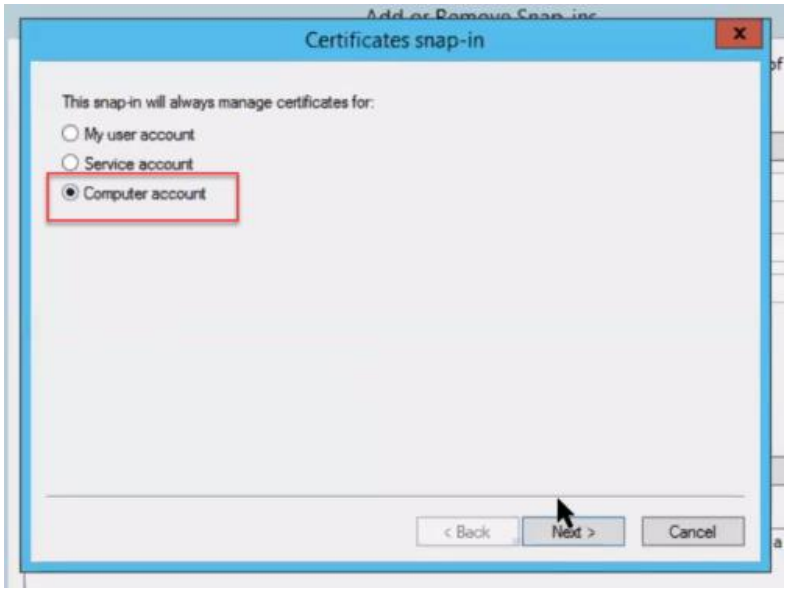
To Generate a Web Server Certificate for the Delinea Privileged Access Service Installation

1. In the server where you're going to install Delinea Privileged Access Service, open the mmc.exe program.
2. In the MMC program, navigate to File > Add/Remove Snap-ins add the Certificates (Computer) snap-in and click Add.



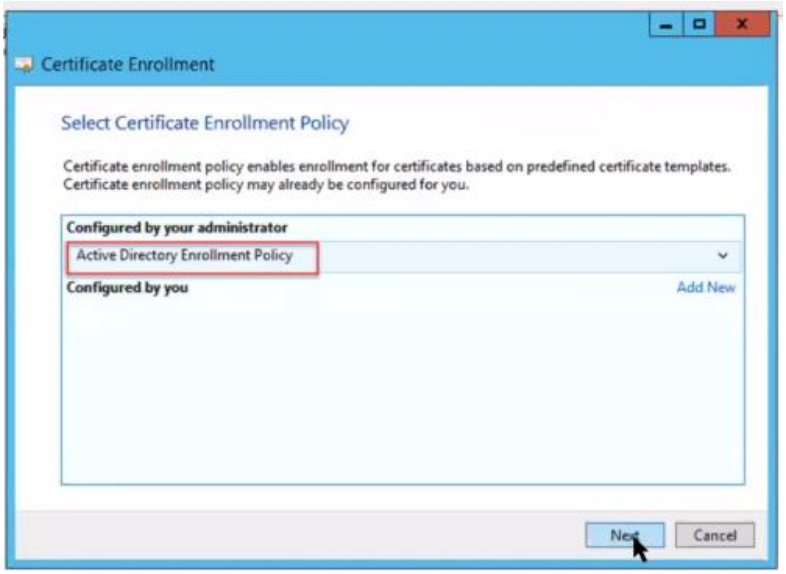
- Add Certificate Snap

3. For Certificates snap-in, choose Computer account and click Next.



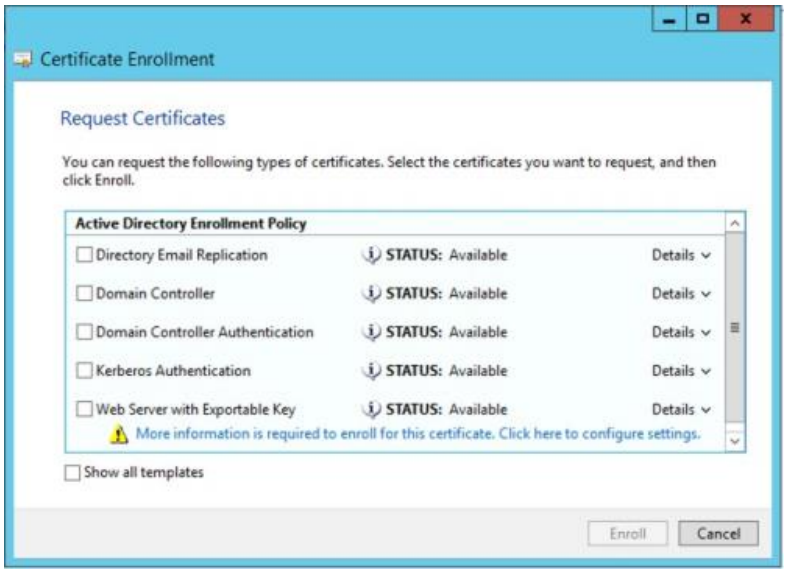
- Computer Account

4. For the Select computer screen, keep all default and click Finish and then click OK.
5. Navigate back to the console, and under Console Root, right-click Personal > All Tasks > Request New Certificate. Click Next on the Certificate Enrollment screen. On the Select Certificate Enrollment Policy screen, ensure you have Active Directory Enrollment Policy and click Next.



- Active Directory Enrollment Policy

6. For Request Certificate, click the checkbox for Web Server with Exportable Key and click the hyperlink directly beneath the selection entitled More information is required to enroll for this certificate. Click here to configure settings.



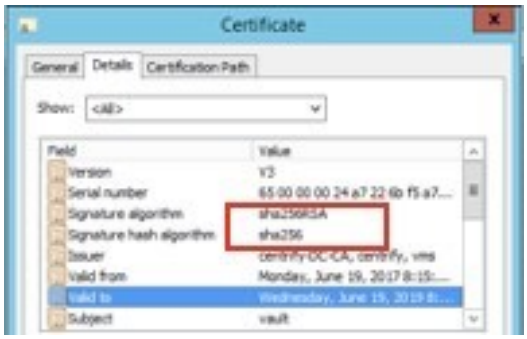
- Click here to configure settings

7. Navigate to Subject, for Subject name, choose Common name. For Value enter the name of the server where you're going to install Delinea PAS and click Add.

   Note: If you are installing Hyper-scalable PAS across multiple servers, provide the FQDN of your PAS installation (example: vault.mydomain.com).

- For Alternative name, choose DNS and then there are two options:
  - Enter *.<your-domain.com> if your web server names will be changing with each upgrade. You will use this option if you are creating new web server machines with each upgrade.
  - Enter the FQDN list of each web server in your cluster if you have a fixed set of web servers that will remain the same after each upgrade. This upgrade process would involve uninstalling the current version on each web server, installing the upgraded package, and keeping the same machine.

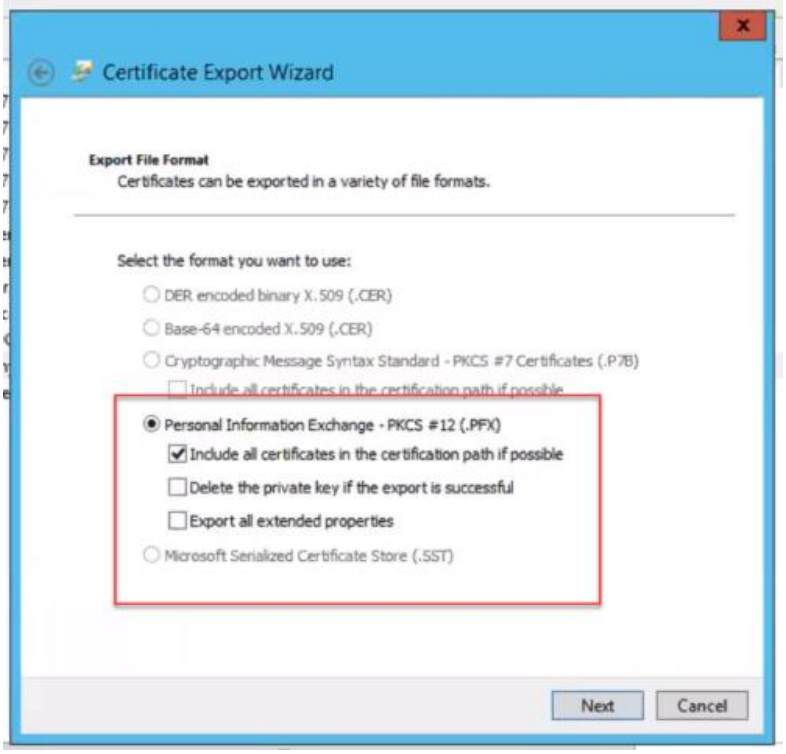
8. Click OK and then Enroll. You should see success.
9. In the Certificates snap-in, navigate to Personal > Certificates and double-click the generated certificate. Navigate to the Details tab, and verify that the algorithm is SHA256 (if you followed the steps in the section above). Scroll down to Subject Alternative name, and verify that the DNS name is *.<your-domain.com>.

- 

- Subject Alternative name
- Keep the Certificates snap-in open for the export process.

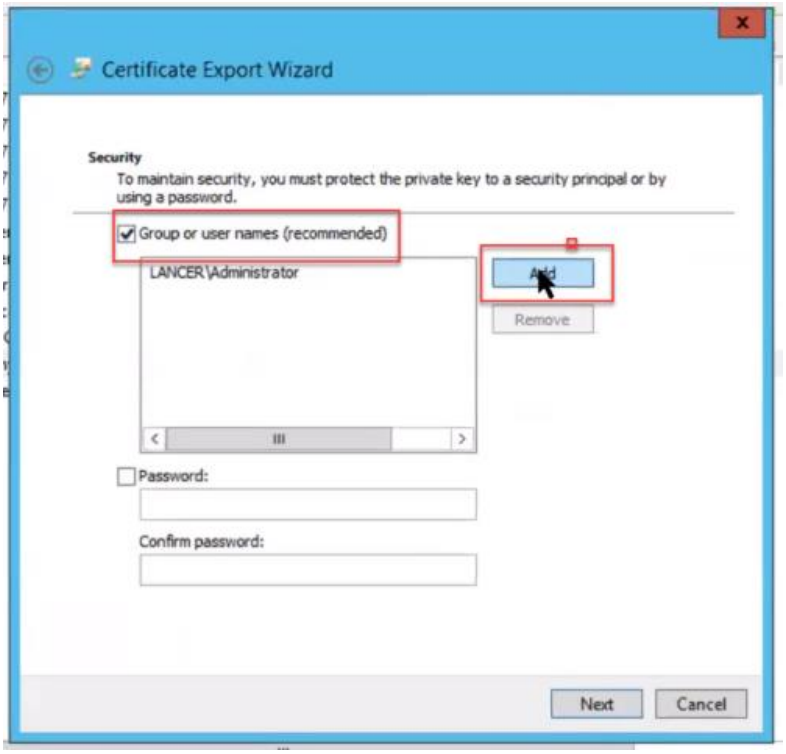
To Export the Certificate with the Private Key

1. Under Personal > Certificates, right click the Delinea (or the name of the server) Certificate and select Export.
2. On the welcome page click Next.
3. On the Export Private Key screen, select Yes, export the private key and click Next.
4. For Export File Format, keep default (Personal Information Exchange - PKCS # 12 (.PFX)) and click Next.

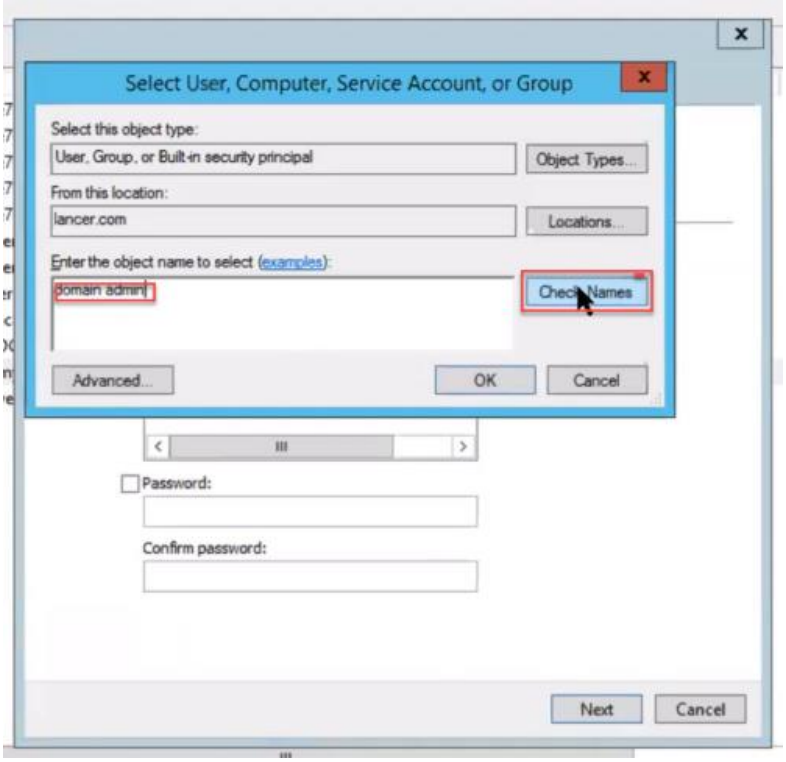


- Export File Format

5. For the Security screen, click the checkbox Group or user names (recommended).

- 

- Group or user names
- Click Add. For the Select User, Computer, Service Account, or Group screen, in the field Enter the object name to select (examples) enter domain admin and click Check Names:

- 

- Select User, Computer, Service Account, or Group
- Click OK and click Next.

6. For File to Export, name the file and click Save.
7. Click Next. Make a note of this location, you'll need it during setup (example: c:\company\company.pfx).
8. Lastly, for the Completing the Certificate Export Wizard screen, click Finish. You will see a screen pop up stating the export was successful. Click OK.

You will provide this file when asked to supply the web server certificate for your installation.

Updating or Replacing a Web Server Certificate

This section explains how to update and replace the web server certificate after it has expired. Before you continue, make sure that you have the new certificate.

Note: Only an experienced HSPAS Admin should perform these steps. For more information about HSPAS, see Introduction to Hyper-scalable Privileged Access Service.

Back Up Before Installing

Before upgrading the certificate, follow the steps below to back up your data (as a precautionary measure):

1. Back up the HSPAS database.
2. Store a copy of the currently deployed certificate on the **Management Node**.
   a. `C:\Centrify\installations\<installation name>\Config`
   b. Make sure the copy is stored where it can be retrieved and not overwritten during an upgrade.
3. Perform a full backup of each node listed below:
   - Web
   - Background
   - Relay
   - Logging
   - Management

   Note: There may be multiple of each of the above nodes that may need to be backed up.
4. If a full backup of each node is not possible, copies of the following data on each node is recommended:
   a. Use `Regedit.exe` to backup the registry folder on each node: `HKLM:\Software\Centrify`.
   b. Backup the following folders on each node:
      i. `C:\Centrify`
      ii. `C:\CentrifyNode`

      Note: Backing up these folders will also include copies of old deployment packages. The `config.json` files and current certificate in use should be part of the management node backup.
5. Copy and save the following value for later use:
   - Current HSPAS host name: Go to `C:\Centrify\installations\<Current HSPAS Host Name>`.

Installing the New Certificate

The following steps cover how to install a new web server certificate after the previous certificate has expired.

To see the prerequisites for certificates see Certificates for Privileged Access Service Authentication.

Verifying Your Certificate

First you need to make sure that your certificate is going to work. You can do that by making sure the filename extension is correct and the subject matches your hostname. Then you will need to save the private key somewhere safe. The steps below show how to verify that your certificate is correct.

1. Capture both the file name and the file extension of the certificate:
   - The extension can either be `.pfx` or `.p12`.
2. Open the certificate and look for **Subject** under **Details**.

- Verify that the current HSPAS host name matches the **Subject** name. The new certificate will not work if they do not match.

3. Save the password associated with the certificate for future use.

Upgrading the Certificate

The following steps will walk you through how to upgrade the web server certificate.

Note: Run this **only** during a maintenance window or downtime.

1. Ensure that the **PostgreSQL** and **Redis** servers are turned on.
2. Log in to the management node as an admin.
3. Copy `<New Certificate>.pfx` to the C:\ folder on the management node.
4. Open an elevated PowerShell Session by clicking **Start Menu** > **Windows PowerShell** > **Run as Administrator**.
5. In PowerShell, change the current directory to `C:\Centrify`
6. Validate that the file '`Centrify-Pas-ModifyInstallation.ps1`' exists in the directory.
7. Run the following PowerShell command:

   ```
   .\Centrify-Pas-ModifyInstallation.ps1 -HostName <Current Host Name> -Certificate <New Certificate path and filename>  -CertificatePassword <Certificate password>
   ```

   For example:

   ```
   Centrify-Pas-ModifyInstallation.ps1 -HostName XYZ.location.current -Certificate C:\NewCertificate.pfx -CertificatePassword 'newPassword'
   ```

   After the command runs successfully, the following message appears:
   `Operations Completed:  Host certificate <old Certificate> replaced with certificate <new certificate>..`

   Note: The above message signifies that the `Centrify-Pas-ModifyInstallation.ps1` command succeeded and the installation is now ready to use the new certificate.

   - When providing the certificate password, place single quotes on either side of it.
     For example:
     `'Password'`
     Otherwise, the password may fail if it contains special characters.
   - You must run all commands from a single PowerShell window.
   - The host name must match the subject name in the certificate. The command above updates the installation configuration with the appropriate certificate information.
   - You may receive a warning when running the PowerShell command, and here's an example of that warning:
     `You've chosen to modify the hostname of the installation for 'pas.my.hspas-dev.net' to the new name of 'change.my.hspas-dev.net' This will mark your current installation under 'pas.my.hspas-dev.net' as deprecated and create a new installation under the name 'change.my.hspas-dev.net' The host certificate and install configuration of your old installation will be copied over to the new installation Finally, this change will update configurations in persistent storage and the FQDN of your installation to the`

`new hostname If you want to proceed with this change, please type 'proceed'.`

After this warning message displays, just enter '`proceed`' and hit the **Enter** key.

8. Verify that the new certificate file now exists in the following location:

   `C:\Centrify\Installations\<Host Name>\config`

9. In the same PowerShell window, run the following command to create a new deployment package with the new certificate:

   `.\Centrify-Pas-NewDeployment.ps1 -HostName <HostName> -ID <Deployment File Name>.`

10. Confirm that the new deployment folder and package exists under the following folder. A deployment package is a zip file:

    `C:\Centrify\Installations\<Host Name>\Deployments\YYYY-MM-DD ID <Deployment File Name>.`

    Note: Here's an example of the deployment folder's name: `2023-02-28 ID 2023CertUpdateDelinea.`

Updating Nodes

The following steps cover how to update different kinds of nodes for your web server certificate.

For each **web node** you are updating, complete the following steps:

1. Open an RDP connection to the node.
2. Copy and paste the `<Deployment File Name>` zip file to the `C:\ drive` on the node.

   For example: `2023CertUpdateDelinea.zip`.

3. Unzip the deployment file in the `C:\` drive.
4. Right-click the deployment file and select **Extract all**.
5. Confirm that the deployment file has been extracted by checking for the new `.pfx` or `.p12` file.
6. Open an elevated PowerShell command on the node:
   a. **Start Menu** > **Windows PowerShell** > **Run as administrator**.
   b. Change the folder to the `C:\<Deployment File Name>` folder.
7. Run the following script:

   `.\Centrify-Pas-Deploy.ps1 -WebNode -RemoveNode.`

   This command removes the node specified on that VM and database reference to the node.

8. Run the following script:

   `.\Centrify-Pas-Deploy.ps1 -WebNode.`

   Note: This process will take several minutes and it will deploy a web node and will set up everything that is needed for the service, including IIS. The script will register this node and add the reference of this node to the database. If you receive an error message stating `Failed to establish a trust relationship`, it means that either the certificate is not trusted, or the hostname does not match the certificate subject name. If this happens, stop the upgrade and fix the certificate.

9. Exit PowerShell.

10. Verify that the process succeeded by going to the website and ensuring it's reachable.
    - Open a web browser and enter the hostname as the URL. If you can see the admin portal login screen, the web node is working successfully.

Updating Different Types of Nodes

1. For each **background node** you are updating, repeat the above steps and replace mentions of 'WebNode' with 'BackgroundNode'.
    - Verify that the background node is running by pressing the **Windows** key, selecting **Services**, and confirming the service '**Centrify Vanguard Background Role**' is listed there and running.
2. For each **relay node** you are updating, repeat the above steps and replace mentions of 'WebNode' with 'RelayNode'.
    - Verify that the relay node is running by pressing the **Windows** key, selecting **Services**, and confirming the service '**Centrify TCP Relay Service**' is listed there and running.
3. For each **logging node** you are updating, repeat the above steps and replace mentions of 'WebNode' with 'LoggingNode'.
    - Verify that the logging node is running by pressing the **Windows** key, selecting **Services**, and confirming the service '**Centrify TCP Relay Service**' is running.
4. After you have updated the above nodes, you must log in to the **management node** as an administrator and complete the following steps:
    a. Open PowerShell command window by going to **Start Menu** > **Windows PowerShell** > **Run as administrator**.
    b. Change the current working directory to `C:\Centrify`.
    c. Run the following:

    ```
    .\Centrify-Pas-SetActiveDeployment.ps1 -HostName <Host Name> -ID <Deployment File Name>
    ```

    > **Note:** This decommissions the nodes running the old deployment and sets the new deployment to active. **New nodes will not respond until their deployment is set as active.**

    d. Run the following:

    ```
    C:/Centrify/Centrify-Pas-NodeList.ps1
    ```

    The above command will list all nodes in the system as well as what deployment they're a part of and if they are active or not.
5. Exit PowerShell.

Verifying the Certificate Works

The following steps will show how to verify your new web server certificate is working properly.

1. Log in to the Admin Portal as an administrator.
2. Enter the hostname in the browser.
   - For example: if `cps-test` is your hostname, you would enter `https://portal.cps-test.com/` into your browser.
3. Confirm that the `SetActiveDeployment` worked. **You will not be able to login into a nonactive deployment**.
4. Verify that the certificate is valid.
   a. Click the lock icon on the top left of the browser's address bar.
   b. Select **Connection is secure** and then select **Certificate is valid**.
   c. Check that the **common name** is the same name as the new certificate.
5. Run a simple job to verify the background nodes, such as changing your password.

   Note: The job will fail if the background nodes are not working properly.

6. Verify that the connectors can reach and communicate with the system to ensure relays are working properly.
   a. Identify all connectors in use by going to **Portal settings: Settings** > **Network** > **Centrify** > **Connectors**.
   b. Restart all connectors.

Changing to a New Database Server or Updating Database Connection Properties

This section describes how to use the `Centrify-PAS-ModifyInstallation.ps1` script to change the database server or to change the credentials used to access the database. For additional script information, see "Centrify-PAS-ModifyInstallation" on page 182.

To Change to a New Database or Update Database Credentials

1. If you are not already logged in to the Management node, log in as a user with administrator rights.
2. At an elevated PowerShell prompt, run `Centrify-PAS-ModifyInstallation.ps1`using the proper parameters to change the database server or to change the credentials used to access the database. Parameters include:
   - `[-DBServer] <String>]` – Enter the new server hostname (URI) for PostgreSQL.
   - `[-DBPort] <String>]` – Enter the PostgreSQL server port, typically 5432.
   - `[-DBUser] <String>]` – Type the new user name required to log in to the database.
   - `[-DBPassword] <String>]` – Type the new password credential required to log in to the PostgreSQL database.
   - `[-DBDatabase] <String>]` – (Optional) Enter the PostgreSQL database name to use when verifying access.

   For example, to change the database and the database credentials:

```
.\Centrify-PAS-ModifyInstallation.ps1
 -DBUser newcentrifyAccount -DBPassword newsecretCode  -DBServer newpostgres.corpnet  -
DBPort 5432
```

3. After updating the database, you must create a new deployment and deploy it to all nodes (TCP Relay Logging if applicable, TCP Relay, Web and Backgroundnodes). Once you create the new nodes, set the new deployment active. For detailed instructions on deploying new nodes, see the following sections:
   - "Phase 3: Creating a Deployment Package" on page 166
   - "Phase 4: Deploying Hyper-scalable PAS software to Web, Background, and TCP Relay Nodes" on page 166
   - "Phase 5: Activating the Deployment" on page 167

Connection String Management

Use the config map section databaseConnections for connection strings with the following keys:

- `Common`
- `Global`
- `GlobalReadonly`
- `Tenant`
- `TenantReadonly`

These keys drive creation of the storage.xml keys and enable you to easily tune of the common connection string.

Changing to a New Redis (cache) Server

This section describes how to use the `Centrify-PAS-ModifyInstallation.ps1` script to change the Installation to use a new Redis server. For additional script information, see "Centrify-PAS-ModifyInstallation" on page 182.

To change to a new Redis server:

1. If you are not already logged in to the Management node, log in as a user with administrator rights.
2. At an elevated PowerShell prompt, run `Centrify-PAS-ModifyInstallation.ps1` using the proper parameters to update the Installation to use a new Redis server. Parameters include:
   - `[-RedisServer] <String>]` – Enter the Redis server hostname (URI).
   - `[-RedisPort] <String>]` – Enter the Redis server port, typically 6379.

   For example, to change the Redis server:

   ```
   .\Centrify-PAS-ModifyInstallation.ps1
   -RedisServer newcache.corpnet-RedisPort 6379
   ```

3. After changing the Installation to use a new Redis server, you must create a new deployment and deploy it to deploy it to all Web and Background nodes. Once you create the new nodes, set the new deployment active. For detailed instructions on deploying new nodes, see the following sections:
   - "Phase 3: Creating a Deployment Package" on page 166
   - "Phase 4: Deploying Hyper-scalable PAS software to Web, Background, and TCP Relay Nodes" on page 166
   - "Phase 5: Activating the Deployment" on page 167

Updating the TCP Relay or TCP Relay Logging Certificate

This section describes how to use the `Centrify-PAS-ModifyInstallation.ps1` script to update the certificate on the TCP Relay node or the TCP Relay Logging node. For additional script information, see "Centrify-PAS-ModifyInstallation" on page 182.

To Update or Replace a TCP Relay or TCP Relay Logging Node Certificate

Note: Relay nodes and logging nodes are treated similarly. The optional logging nodes can be upgraded using the same procedure as relay nodes.

1. If you are not already logged in to the Management node, log in as a user with administrator rights.
2. At an elevated PowerShell prompt, run `Centrify-PAS-ModifyInstallation.ps1` using the proper parameters to update or change the TCP Relay or TCP Relay Logging node certificate.

Parameter	Description
TCP Relay node: [-NewRelayCertificate]	Use this parameter to generate and configure a new security certificate for TCP Relay nodes. For example: .\Centrify-PAS-ModifyInstallation.ps1 -NewRelayCertificate
TCP Relay Logging node: [-NewLoggingRelayCertificate]	Use this parameter to generate and configure a new security certificate for the TCP Relay Logging node. For example: .\Centrify-PAS-ModifyInstallation.ps1 -NewLoggingRelayCertificate

3. After updating the certificate, reboot the Web and Background nodes.

Backup and Disaster Recovery

In the event of a failure, you can fully restore Hyper-scalable PAS by recovering or restoring the PostgreSQL data, ensuring a Redis server is also available, building a new Deployment and deploying it, and then setting the Deployment to active. To restore Hyper-scalable PAS, perform the steps below.

Determining How to Restore Hyper-scalable PAS

- If the database is still intact and both it and the Redis server are still at their original URIs, you can reuse the last Deployment package to create as many Web and Background nodes as needed. For steps on how to reuse the Deployment package, refer to the section *Deploying Hyper-scalable PAS software to Web, Background, and TCP Relay nodes* under "Installing Hyper-scalable PAS" on page 163.
- If the database has been corrupted or destroyed, but both the database and Redis servers are still using the same URI, restore the database and then reboot the node servers. Hyper-scalable PAS should recognize the database and resume service.
- If the database or Redis URIs have changed, do the following:
  1. Update URIs using `Centrify-PAS-ModifyInstallation` script to update the certificate. To do this, see "Updating the TCP Relay or TCP Relay Logging Certificate" on the previous page.
  2. Create a new deployment: `Centrify-PAS-NewDeployment`.
  3. Deploy it.
  4. Change the active deployment.

Manually Rebuilding and Restoring Hyper-scalable PAS

To manually rebuild and restore a Hyper-scalable PAS instance, perform the following steps:

Note: Manual back up and restore is your responsibility and is not performed in any way by Hyper-scalable PAS.

1. Restore your latest backup of the PostgreSQL data to the new database server. Find the URIs and credentials for both the Redis and PostgreSQL servers.
2. Run `Centrify-PAS-ModifyInstallation` with parameters for what has changed. For example, if the certificate has not changed, you do not need certificate parameters. Alternately, for example: if the database host has changed, you must provide all database parameters. The parameter options are mostly identical to `Centrify-PAS-NewInstallation.` The only exception is `-Config`, which is not accepted.
3. Create a new Deployment package by running the `Centrify-PAS- NewDeployment.ps1` command on the Management node.
4. Copy this Deployment to new Windows Server nodes and install (using command `Centrify-PAS-Deploy`) new Web, Background, and TCP Relay nodes.
5. From the Management node, activate the Deployment using the `Centrify-PAS-SetActiveDeployment.ps1` command. Pass in the Deployment ID that you either set as a parameter or received as output from the `Centrify-PAS-NewDeployment.ps1` script.
6. Ensure that the load balancer can send traffic to the Web nodes.
7. On the Management node, list out the nodes (using command `Centrify-PAS-NodeList`) and forcibly remove (using `Centrify-PAS-ForceRemoveNode`) any nodes from previous Deployment IDs that no longer exist or cannot talk to the database.

Maintaining a Snapshot

As a method of backup, it is important to maintain an accurate snapshot of your VMs. The following comprise a snapshot for Hyper-scalable PAS:

- A copy of the "Installing Hyper-scalable PAS" on page 163 you created during the installation process.
- A copy of a regular full pg_dump of the PostgreSQL database.

Migrating On-Premise PAS to Hyper-scalable PAS

This document describes how to move your data from On-Premise PAS database to Hyper-scalable PAS (also referred to as Hyper-scalable PAS) database. The migration process requires you to run the migration scripts to gather configuration and database data from the On-Premise PAS server and then build a Hyper-scalable Privileged Access Service installation using the migrated configuration and database data.

Note: The migration disables the On-Premise PAS server to prevent data corruption. It is critical that the On-Premise PAS server remains disabled; otherwise data and account corruption may occur. The Privileged Access Service is not available until the entire migration and deployment process is complete (in other words, there is a period of downtime during which the Privileged Access Service is unavailable).

Prerequisites

You will need the following in order to perform the migration procedures:

- Full access with administrative rights and the ability to run PowerShell scripts to the On-Premise PAS server.
- Minimum software and hardware requirements for deploying Hyper-scalable PAS. See the *Installation and Configuration Guide for Hyper Scalable Privileged Access Service* for specific details.
- Migration scripts: `Centrify-PAS-PrepareOnPremMigration.ps1` and `Centrify-PAS-InstallationFromOnPremMigration.ps1` (These scripts come with the Hyper-scalable PAS software package)
- Hyper-scalable PAS software package: install.ps1, `CentrifyPlatform[Build.Number].zip`

  Note: Hyper-scalable PAS may need to use the same database server operating system as On-Premise PAS, as PostgreSQL retrieves (anduses) the collation/character type settings from the On-Premise PAS host operating system.

  For example, the LC-COLLATE value, **English_UnitedStates.1252**, is roughly the Windows PostgreSQL equivalent of **en_US.UTF-8** on some Linuxdistributions, both with Encoding set to UTF8. PostgreSQL cannot discernthat they are functionally similar however, so it lacks trivial portingbetween them. Consequently, to migrate to Hyper-scalable PAS withpre-existing data, you need to ensure the same localization settings are available on the new database server by using the same database pod.

Migration Overview

The following is an overview of the steps required to migrate from On-Premise PAS to Hyper-scalable PAS.

- Install a Hyper-scalable PAS Management node.
- Verify that you have the migration preparation script and the migration installation script in the C:\Centrify\Migration folder on the Managementnode (`centrify-PAS-PrepareOnPremMigration.ps1`) and`centrify-PAS-InstallationFromOnPremMigration.ps1`.
- Copy the migration preparation script (`centrify-PAS-PrepareOnPremMigration.ps1`) from the Management node to your current On-Premise PAS server.
- Prepare the On-Premise PAS server for migration.

  For a standard migration, you need to perform the following steps on the On-Premise PAS server (if you have an external databaseconfiguration you only need to perform the shutdown cluster step in the Failover Cluster Manager):

  - In the Failover Cluster Manager, remove the disk from the role and the cluster
  - Shutdown the cluster
  - Bring the cluster disk that contains the database information online
  - Start the On-Premise Infrastructure Services database

    Note: As stated above, for external database configurations, you only need to perform the shutdown cluster step, then you can run the `.\Centrify-PAS-PrepareOnPremMigration.ps1` script.
- From the On-Premise Infrastructure Services server, run the migration preparation script to package the data needed for migration.

  To avoid the possibility of inconsistent data, the On-Premise Infrastructure Services server is disabled.
- After running the migration preparation script, copy the directory results to the Management node.
- Run the `Centrify-PAS-InstallationFromOnPremMigration.ps1` script in the Management node Migration directory, specifying the directory where you copied the On-Premise PAS data, to create an Installation.

At this point the migration is complete and you need to continue with Hyper-scalable PAS deployment as described in the *Installation and Configuration Guide for Hyper Scalable Privileged Access Service*. You will need to:

- Create a deployment
- Deploy Windows servers to create Logging (if desired), Web, Background and

  Relay nodes
- Update the Load Balancer and set the new deployment active

Detailed Migration Procedures

Important: To avoid synchronization issues, such as passwords or credentials becoming out-of-sync and disabling account access, the On-Premise PAS server must be shut down when the migration preparation script is started, and must not be restarted. If you are running Windows Clustering, shut the entire cluster down and do not restart it. Only one On-Premise PAS server should be active prior to running the migration preparation script. After the migration no On-Premise PAS servers are active.

All PowerShell sessions must be elevated (RunAs Administrator).

The following instructions are also available in the *Installation and Configuration Guide for Hyper Scalable Privileged Access Service*. Refer to that document for additional details.

Installing the Management Node

1. Download/copy the Hyper-scalable PAS software package from Delinea to the Windows server you have designated to be the Management node.

   The installation package includes the following software components: `install.ps1,centrifyPlatform [Build.Number].zip`
2. Open an elevated PowerShell session and run the `install.ps1` script to create the Management node.

   This expands and installs the `centrifyPlatform[Build.Number].zip` (you can optionally set the target directory with the `-target` parameter). The defaultdirectory is C:Delinea). Once completed, the necessary scripts are available on the Management node for installation and deployment.

   For detailed instructions, see the *Installation and Configuration Guide for Hyper Scalable Privileged Access Service* documentation.

Copying the Migration Preparation Script

Copy the `centrify-PAS-PrepareOnPremMigration.ps1` script from the C:\Centrify\Migration directory on the Hyper-scalable PAS Management node to your On-Premise PAS server.

The destination location of the script on the On-Premise PAS server doesn't matter as long as you can read and write to that location.

Preparing the On-Premise PAS Server for Migration

For standard migrations running Windows clustering:

To ensure data synchronization and that the On-Premise PAS server database is accessible, you need to perform all of the following tasks in the Windows Failover Cluster Manager before running the migration script.

For migrations that use an external database:

If your configuration uses an external database, you only need to perform steps in the *Shutdown the cluster* section below before running the migration script.

Note: The following procedures are performed on the On-Premise PAS server.

Remove the disk from the role and the cluster:

1. Access the **Windows Server Manager > Tools > Failover Cluster Manager**, then navigate to the cluster resource.
2. In the Failover Cluster Manager, expand the cluster name and navigate to

   Storage > Disks.
3. Right-click the disk and select **Remove from role** and then select **Yes**

   at the confirmation screen.

4. Right-click the disk again and select **Remove** and then select **Yes** at the confirmation screen.

Shut down the cluster:

This step is required for both standard and external database migrations.

1. In the Failover Cluster Manager, right-click the cluster name and select **More Actions > Shut Down Cluster...**
2. Select **Yes** at the confirmation screen.

Bring the cluster disk that contains the database information online:

1. Navigate to the Windows Disk Management screen.
2. Right-click the disk and then select **Online** from the menu.

Start the On-Premise Infrastructure Services database:

1. In Windows, navigate to **Administrative Tools > Services**.
2. Locate the service Identity Service Database
3. Right-click the service and select **Start**.

Running the Migration Preparation Script

1. From the On-Premise Infrastructure Services server, run the `centrify-PAS-PrepareOnPremMigration.ps1` script to package the data needed for migration.

   By default the migration data is copied to C:\OnPremData. If necessary, you can change the destination of the output directory.
2. Enter Disable Server when prompted to continue.

   This disables the On-Premise PAS server; making the Hyper-scalable PAS inaccessible. Do not re-enable the On-Premise PAS server, asthis could result in Hyper-scalable PAS data getting out-of-sync. Instead,complete the steps in this *Migration Guide* to enable Hyper-scalable PAS Web Nodes and set the Deployment to Active.

Copy the On-Premise PAS Data to the Management Node

Copy the entire contents of the On-Premise PAS server C:\OnPremData (or as specified) folder to the Management node. This includes two SQL files and one ZIP file. The files must go into a single directory on your Management node.

Create the Installation from the Migrated Data

From the Management node, in the C:\Centrify\Migration directory, run the `centrify-PAS-InstallationFromOnPremMigration.ps1` script.

The migration installation script has similar requirements to the standard `centrify-PAS-NewInstallation` script, with a few differences:

- `-MigrationDirectory` - points to the directory with the three files from the On-Premise PAS migration
- No need for the administrative user credentials, as those are migrated with the other data

Troubleshooting

The following are Hyper-scalable Privileged Access Service frequently asked questions and information about specific features and functionality as follows:

- Scripts won't run.
- Unknown or non-existent node listed in NodeList.
- Web node is installed but site does not appear.
- What is the Logging Relay?
- How to retrieve Node Logs
- How to retrieve Connector Logs without a Logging Relay
- How to provide a Support Report

Scripts Won't Run

If you receive an error such as:

Message: File <file name> cannot be loaded. The file <file> is not digitally signed. You cannot run this script on the current system. For more information about running scripts and setting execution policy, see about_Execution_ Policies at http://go.microsoft.com/fwlink/?LinkID=135170.

+ CategoryInfo : NotSpecified: ([Write-Error], WriteErrorException

+ FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,Centrify-Pas-Deploy.ps1

Review "PowerShell Execution Policy" on page 153 for more information.

Unknown or Non-existent Node Listed in NodeList

If you see nodes that no longer exist listed when you run Centrify-PAS-NodeList.

Common Cause

The Node was destroyed, lost, or it was unable to connect to the database when it was deprovisioned using `Centrify-PAS-Deploy -RemoveNode` on the node itself.

Solution

`Centrify-PAS-RemoveNode` from the Management node will remove the node from the database.

Web Node is Installed But Site Doesn't Appear

After you have deployed a web node using `Centrify-PAS-Deploy -WebNode`, set it active, browsing to the host name doesn't work.

Common Causes

There are several possibilities:

The name is not registered

To browse to the Web node, the host name must be registered with the appropriate name server. To verify this, from your client system, enter:

```
nslookup <hostname>
```

Example:

```
nslookup pas.corpnet.com
```

The return IP address should match the public IP address of the node or the node's load balancer.

For example:

```
PS C: \> nslookup pas.corpnet.com

Server: dns.google

Address: 8.8.4.4

Non-authoritative answer:

Name: corpnet.com

Address: 108.167.88.99

Aliases: pas.corpnet.com
```

This tells us that:

1. Name Servers (in Windows Control Panel) are set to Google's DNS (8.8.4.4).
2. Pas.corpnet.com is listed and has a public IP address (meaning: not 192.168.*.* or 10.0.*.*).

If, instead, we got:

```
PS C:\ > nslookup pas.corpnet.com
Server: dns.google
Address: 8.8.4.4
*** dns.google can't find pas.keybounce.com: Non-existent domain
```

This indicates that the name could not be resolved. Ensure it is plugged into the correct authoritative name server, such as AWS' Route53, or GoDaddy, and so on.

Note: This address is not the internal address of the Web node(s), but rather the public internet-facing port for the Load Balancer or Firewall.

Inaccessible IP Address

If the listed address from the above step comes back as a Private IP address or in any of the following ranges...

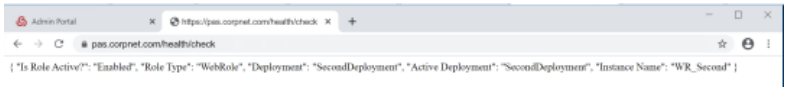
- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

...the IP Address is not accessible from the outside world. It needs an external public (generally static) IP Address. The IP address is not for the Web node, unless there is only one Web node (not recommended), but rather for the Load Balancer.

Load Balancer Health Check Fails

Once you have verified that the name resolves to the Load Balancer, ensure the Load Balancer can see healthy web nodes.

- The Health Check point is /health/check. You should see all web nodes listed and at least those on the current deployment (`Centrify-PAS-SetActiveDeployment`) displaying “healthy”.
- If you do not see any Web nodes, check your load balancer configuration.
- If you see the correct Web nodes, but they display as “unhealthy,” verify that they are on the correct deployment. Navigate to the Web node by namefrom the node (this will generally work as the deployment process adds thename to the local hosts file at `c:\Windows\System32\Drivers\Etc\hosts`) or IP Address, adding the “/health/check” path.



In this case, we see that the Role is **active**, with the Instance Name of “WR_Second.” If the Web nodes list as **offline**, ensure they are powered up and booted.

- From the Management node, ensure the Web node is listed as **online** and **active** from `Centrify-PAS-NodeList.`
  - If it is offline, it is not accessing the database and may not be running.
  - If it is online but inactive, it has the wrong deployment ID. You need to either change the active deployment with `Centrify-PAS-SetActiveDeployment` or you will need to deploy a node of the correct deployment.
- RDP into the Web node and verify that IIS is running and that there is a `c:\CentrifyNode` directory.

Note: If the above are not the case, it may be necessary to re-image and re-deploy this Web node.

What is the Logging Relay?

The Logging Relay provides several features including the following:

- Aggregates logs from all deployed Web and Background nodes, providing a single place to retrieve them.
- Enables the Management Node to watch the logs, using LogWatcher (Centrify-PAS-WatchLogs).

In addition to being essential for trouble-shooting, the output provided by a Logging Relay plus LogWatcher can be fed into a custom or Splunk-like parser to generate real-time analytics and alerts.

How to Retrieve Node Logs

On the Logging Node, you can find the logs at `c:\Centrify\Logs`. Their names contain the date ranges and log type.

For example, for an installation with a hostname (URL) of pas.corpnet.com, generated from the hours of 9:00pm - 11:59pm on May 14, 2020, the log names will look similar to the following:

- 2020-05-14-21-pas.corpnet.com-navel.log
- 2020-05-14-21-pas.corpnet.com.log
- 2020-05-14-22-pas.corpnet.com-navel.log
- 2020-05-14-22-pas.corpnet.com.log
- 2020-05-14-23-pas.corpnet.com-navel.log
- 2020-05-14-23-pas.corpnet.com.log

The plain .log files have standard log data in them, while the -navel.log files are not human-readable, and contain timing data about internal operations that help Delinea determine where a task might be taking longer than expected.

For convenience, you can use `Centrify-PAS-GetDiags.ps1` on the Logging Node to specify a start date, start hour, and duration (hours) for the run. This will package the logs from all nodes and the connector logs.

How to Retrieve Connector Logs without a Logging Relay

The documented process is to install a Logging Relay prior to installing any other nodes.

Note: Delinea cannot guarantee support of an installation that did not follow the documented process.

If your Logging Relay is not available for some reason, `Centrify-PAS-GetDiags` can also be run from the Management Node. You can only retrieve connector logs using this method since the Management node can't reach the Web or Background Node logs.

How to Provide a Support Report

In addition to logs, basic information about the installation and environment can help Delinea quickly find the cause of most reported issues.

The Support Report includes information about all deployed nodes, the versions of the database and binaries installed, and various run-time data including:

- Delinea connectors, including current status and latency.
- `CurrentDeploymentId`
- `DatabaseConnections`. This is for debugging database issues. There is no PII in this.
- `DeploymentHistory` and `SchemaHistory`, including binary (cloud) versions.
- Running and Queued Jobs. In a healthy system, this is usually empty or nearly empty.
- Nodes including type, name, and the basic environment.
- `StatSnap`. These are scale statistics. For example, the count of (but not enumeration of) devices, entitlements, systems, etc.

  Note: None of this information expose any confidential data, but you may still want to scan over the information prior to submitting.

Delinea cannot retrieve this information directly, unless you provide explicit remote access and permission. The information can only be generated using one of the following methods:

- In the Admin Portal, using the **Support** menu located in the upper right

  area of the screen.
- By calling the /health/SupportInfo endpoint. For example, with CCLI.
- By running `Centrify-PAS-NodeList.ps1 -Support` on the Management Node.

Enabling Certificate Authentication by Smart Card and Tenant CAs

The setup_certauth.ps1 script is provided with the Delinea Privileged Access Service to enable certificate authentication when client certificates are issued by Delinea or by your own certificate authority.

After you execute setup_certauth.ps1, the Certificate Authorities feature located in the Admin Portal **Customization > Settings > Authentication** page is enabled. In the Certificate Authorities page, you can configure authentication by smart card and by certificates issued by your PKI infrastructure. If you do not execute setup_certauth.ps1, the Certificate Authorities feature located in the Admin Portal **Customization > Settings > Authentication** page remains disabled, and is not visible.

Before you can execute setup_certauth.ps1, you must ensure that the following prerequisites are met:

- A CNAME record that points the DNS host to the Delinea PAS host has been created within your DNS infrastructure. After the CNAME record is created, it can take up to 15 minutes for the CNAME to resolve the IP addresses of the DNS host and the Delinea PAS host.
- A certificate from a trusted certificate authority has been issued for the DNS host. When the setup_certauth.ps1 script runs, you will be prompted to specify the path to this certificate.

The setup_certauth.ps1 script validates these prerequisites during runtime. If either prerequisite is not met, setupcertauth.ps1 aborts.

To enable authentication by smart card and tenant CAs:

1. On the computer where the Delinea PAS is running, open a PowerShell console window as Windows administrator.

2. In the PowerShell console, change to the Delinea PAS scripts folder. The scripts folder is located in the installation folder that was specified during Delinea PAS installation. If the default installation location was selected, the scripts folder is in 'C:\Program Files\Centrify\Centrify Identity Service'.
3. From the scripts folder, run the setup_certauth.ps1 script:'.\setup_certauth.ps1'
4. When the script prompts you to verify that the prerequisites are satisfied, type **Y** and press **Enter**.
5. The script validates prerequisites, and prompts you for the path to the DNS host certificate. Type the path to the certificate and press **Enter**.

When the script finishes, the Certificate Authorities feature is located in the Admin Portal **Customization > Settings > Authentication** page is enabled.

Deploying Customer-Managed (On-Premises) PAS

The customer-managed (on-premises) Privileged Access Service deployment model is an on-site solution where you provide your own servers as part of the infrastructure solution. The infrastructure you choose can be either an internal protected network, a private cloud, or a public cloud instance.

Managing User Access

Privileged Access Service provides a secure platform for managing privileged access and an ecosystem for producing adaptive analytics, auditing of user activity, and built-in and custom reports. As a key component of that ecosystem, user access forms the foundation for all other services and features.

Users and Roles

Admin Portal roles are sets of user accounts. You use roles to assign applications, permissions, and policies to sets of users. Users can be members of multiple roles.

Privileged Access Service provides two predefined roles:

- System Administrator
- Everybody

The account that is created automatically at tenant creation is an Privileged Access Service service user account and is automatically made a member of the System Administrator role with all administrative rights. Roles control what different sets of users can do and you can add roles to define the policies that apply to different groups of users.

By default, all new Privileged Access Service users are added to the Everybody role. Members of the Everybody role are automatically granted permission to access to the Admin Portal. If you have some users that are not included in the Everybody role, however, you must explicitly deploy the Admin Portal application to the role where those users are members.

The Privileged Access Service assigns applications and applies the selected administrative rights to all role members. For example, if you add an Active Directory/LDAP group to a role, the applications assigned to that role are now available to members of that group. Similarly, when you remove a user from a role, the Privileged Access Service deletes all the web applications assigned to that role from registered devices.

Changes that impact the assigned applications or administrative rights will take effect when the user next logs in to the device. You can push the changes to the users for immediate update by selecting the role members on the Users page and sending the **Reload** command.

See "Predefined Roles" on page 276 for a list of predefined roles.

Your role must have the Roles Management administrative right to add and modify roles. See "Creating Privileged Access Service Administrators" on page 276.

Adding Roles

Privileged Access Service provides two predefined roles by default: **Everybody** and **System Administrator**. Initially, only the members of the System Administrator role have the full rights to perform all administrative tasks. If you want to delegate full administrative activity to other users, you can add them to the predefined System Administrator role.

All other users are added to the Everybody role by default.

In most organizations, however, the two default roles do not provide enough granular control over who can do what or which policies should be applied to different groups of users, so additional roles are necessary. You can create as many additional roles as you need.

You can add roles before or after you add directory service users. If you plan to delegate some administrative activity to other users, you might want to create the roles with specific administrative rights before you add users to the service.

If your users assigned to the role will be accessing enrolled Linux systems, you can specify the Unix Profile information, if desired. You can map a role to either a local group that already exists on systems or a new local group.

To Add a Role

1. In the Admin Portal, click **Access** > **Roles**.
2. Click **Add Role**.
3. Enter the role name and an optional description.

   Click **Save** to continue.
4. Click **Members** > **Add** to add users to the role.

   You can add directory service users and external identity store users. If you are preparing a role with administrative rights before adding or inviting users, you can add the appropriate members later.
5. Click **Administrative Rights** > **Add**.
6. Select the check box associated with each right you want to assign to the role, then click **Add**.

   For a description of the administrative rights, see see "Admin Portal Administrative Rights" on page 277
7. If you want the members of this role to be able to access Unix/Linux systems, go to the **Unix Profile** page and select **Map role as a group on enrolled systems**.

- **Unix name**: This is the name of the new or existing local group. You must specify this field.

  Enter an existing local group name if you want to map this role to a group that exists already on your Linux systems.

- **GID**: This field is optional. If you are mapping this role to an existing local group, be sure to enter the correct GID (otherwise the mapping won't work correctly).

8. Click **Save**.

Adding Privileged Access Service Users

Typically, the account you use to log on for the first time is the default administrative account for the Privileged Access Service with full administrative rights. See "How to Update the Default Administrator Account" on page 248 for information on how this default account is created.

Using the default administrative account, you can create additional directory service users one-at-a-time or you can perform a bulk import of up to 10,000 users from an Excel xls/xlsx spreadsheet or a comma-separated values (CSV) file.

Directory Service Users and Roles

Privileged Access Service provides two predefined roles:

- System Administrator
- Everybody

The account used to log on for the first time is a Privileged Access Service service user account and is automatically made a member of the System Administrator role with all administrative rights. Roles control what different sets of users can do and you can add roles to define the policies that apply to different groups of users.

By default, all new Privileged Access Service service users are added to the Everybody role.

Roles are a key element for all of the Privileged Access Service you choose to deploy. For example, the Privileged Access Service assigns applications and applies administrative rights based on role membership. For more information about how role membership affects user access and how policies are applied, see "Adding Privileged Access Service Users" above.

If all of your users are going to be Privileged Access Service users, the next step is to begin adding account information for those users to the Privileged Access Service service.

If you are using another identity store—such as Active Directory or another LDAP-based service—for all or some of your user accounts, the next step is to install a connector to point to that identity store. For more information about installing a connector, see Installing a Delinea Connector. For more information about using different identity stores, see "Selecting an Identity Repository" below.

Selecting an Identity Repository

Privileged Access Service requires an identity repository for storing user data and authenticating these users. You can use either or both of the following:

- Delinea Directory: Privileged Access Service includes this built-in identity repository. With this option, we use the Privileged Access Service account to authenticate users and, if you are using the Privileged AccessService for mobile device management, to store the registered device records.
- Active Directory/LDAP: Privileged Access Service securely connects with your existing Active Directory/LDAP infrastructure through the Delinea Connectorto authenticate users when they log in to the web portals and registerdevices. Privileged Access Service does not replicate Active Directory/LDAP accounts or attributes in the Privileged Access Service.

If your organization is heavily invested in Active Directory/LDAP, you can continue to use it as your primary identity store and use the same tools (for example, Active Directory Users and Computers) to manage users and mobile devices.

You can use both identity stores simultaneously, too. For example, if you decide to use Active Directory/LDAP as your primary identity store, the Privileged Access Service can provide a convenient supplemental repository for the following types of users:

- Emergency administrators: If there is ever a network break down to the Active Directory domain controller, no one with just an ActiveDirectory/LDAP account can log in. However, if you create administratoraccounts in Privileged Access Service, these users can log in to Admin Portal launch web applications.
- Temporary user: Some organization's security policy can make adding a short-term user to Active Directory/LDAP a complex and time-consuming task.If you have a temporary worker who needs access to just the applications youdeploy through the Privileged Access Service, it may be simpler to add the account to Privileged Access Service.
- Contractors or less-trusted users: Sometimes you do not want users to have the full set of privileges and access rights an Active Directory/LDAPaccount provides. In this case, you create the account in the Privileged Access Service only.

To avoid users logging in to unintended repository accounts and other account related confusion, we recommend that you do not create duplicate accounts (same user name/password) in both the Delinea Directory and Active Directory/LDAP.

Creating Individual Directory Service Users

Initially, you might want to create individual directory service users one at a time directly in the Admin Portal. For example, you might want to add another directory service user that will be assigned to the System Administrator role or delegated to perform user management or role management tasks but not other administrative tasks.

To create user accounts one at a time

1. Log in to Admin Portal using your administrator account.
2. Click **Access** > **Users** > **Add User**.
3. Enter a login name and select a suffix.

   A user name can be composed of any of the UTF8 alphanumeric characters plus the symbols + (plus), - (dash), _ (underscore), and . (period).

The suffix is the part of your account name that follows “@”. For example, if your account name is bob.smith@acme.com, then the suffix is acme.com. Bydefault, the suffix associated with your default account is populated. See"How to Use Login Suffixes" on page 236 for more information on suffixes.

All login suffixes are displayed in the list, including the login suffix for any Active Directory/LDAP domains you are using.

Important: If you select the login suffix for an Active Directory/LDAP domain, the account is not added to Active Directory/LDAP. The account’sSource column will indicate Privileged Access Service as the source, rather than Active Directory/LDAP.

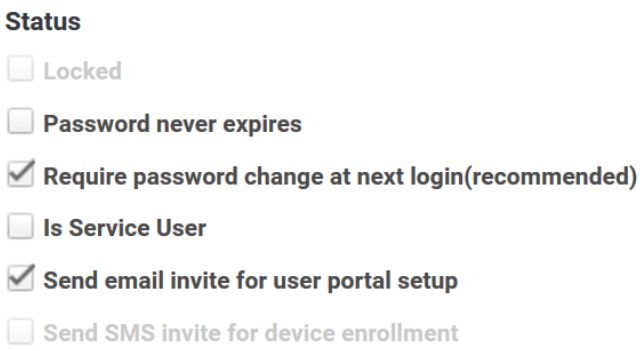
4. Enter the email address and display name for the user.
5. Enter a password.

   This is a one-time password for the user to log in to Admin Portal when you select “Require password change at next login (recommended)” in the Status settings. This password is replaced with the password created by the user.

   The default minimum password requirements are:

   - 8 characters
   - 1 numeric character
   - 1 upper case letter
   - 1 lower case letter

   See "How to Specify User Password Complexity Requirements" on page 239 to change the default requirements.
6. Select the appropriate Status settings.



   You can customize the email message sent when you invite users–see "How to Customize Email Message Contents" on page 251.
7. (optional) Enter the appropriate information for the Profile fields.
8. (optional) Enter the appropriate information for the Organization field.
9. Click **Create User**.

A notification will be sent to the newly created user using your selected method.

Using the Bulk User Import Wizard to Add Privileged Access Service Accounts

After you create the file, use the Bulk User Import wizard to create the accounts.

To add Privileged Access Service accounts using the Bulk User Import wizard:

The procedure assumes you have already created the Excel or CSV file.

1. Log in to Admin Portal
2. Click **Settings** > **Users > Bulk User Import > Browse**.

3. Navigate to the file.
4. Click **Open > Next**.
5. Review the entries.

   The first 15 records are displayed. Use this display to ensure you have formatted the entries correctly.
6. Click **Next**.

   The Delinea Directory - Bulk Import Report field is automatically populated with your email address. Change the address if you want the email address to go to someone else.
7. Click **Confirm**

After the wizard completes the import, the Privileged Access Service sends two email messages:

- A Delinea Directory - Bulk Import Report. This email message is sent to the email account that you had specified to receive the report. It indicates how many new users were specified in the file and how many were successfully added. An explanation is provided for each failed account.
- A Delinea Directory - New User Account. This email message is sent to each user account created. The message includes a link to the Admin Portal and a one-time password. When users open the link, they are prompted to create a new password (unless you have configured otherwise).

  Note: You can customize this letter–see "How to Customize Email Message Contents" on page 251.

How to Bulk Import User Accounts

You use an Excel spreadsheet or CSV file in conjunction with Admin Portal to bulk import Delinea Directory user accounts. The user account file can contain up to 10,000 accounts.

You should run bulk user import after you have assigned the web applications to the roles. The Privileged Access Service sends the login email message to the new users immediately after creating the account. If you do

not have the applications assigned, the users are presented with an empty Apps screen when they log in to the Admin Portal.

To create the file, use the CSV file template provided (Option 1 in the import wizard) or create the file from scratch. Ensure that your user account file follows these guidelines:

- The required fields must be present.
- Each field must have a header.
- Headers must match exactly as shown in the following table, including upper case characters and spaces.
- Fields/Attributes not listed in the following table must be defined in **Settings > General > Additional Attributes**. If the additional attributes are not defined, they will not be uploaded. The attribute names you define on the Additional Attributes page must exactly match the corresponding headers in the CSV file.

Default Fields	Rules
Login Name	Required Enter the full user name, including the login suffix in the form <login name>@<loginsuffix> The login suffix must exist already.
Email Address	Required You can specify one email address only. The email address must be of a valid form. Plain text strings, such as “N/A” or “unavailable”, will be rejected.
Display Name	Optional You can enter the display name in Excel using either format: first last last, first If you are editing the CSV file, use quotes if you specify the last name first (for example, “last, first”).
Description	Optional Do not use punctuation. Limit is 128 characters.
Office Number Mobile number Home number	Optional You must enter the area code. You can enter domestic US numbers in the following forms: 1234567890 123-456-7890 Use E.164 number formatting to enter an international number. If you are using the phone or text message options for multifactor authentication, the Office and/or Mobile numbers must be accurate or the user will not be able to log in.
Roles	Optional All accounts are automatically added to the Everybody role. You can specify multiple roles. Use a comma to separate each role. If you are editing the CSV file, surround the roles with quotes–for example: “role1,role2,role3”. The role must already exist, and the names are case sensitive.
Expiration Date	Optional Enter a date when the account expires. If you do not set a date, the account does not expire. This field is not in the CSV template.
Password	Optional Sets the password for the user. Password requirement is based on the password policy settings in **Admin Portal > Policies > User Security Policies > Password Settings**.

Default Fields	Rules
Require Password Change	Optional Specifies if users must change the password upon the first successful login. The supported inputs are: `False`, `f`, `no`, `n -- No password change required`, `True`, `t`, `yes`, `y -- Password change required`
Reports to	Optional Name of the reporting manager. This field is not in the CSV template.

Using the Bulk User Import wizard to add Privileged Access Service accounts

After you create the file, use the Bulk User Import wizard to create the accounts.

To add Privileged Access Service accounts using the Bulk User Import wizard:

The procedure assumes you have already created the Excel or CSV file.

1. Log in to Admin Portal
2. Click **Settings** > **Users > Bulk User Import > Browse**.

3. Navigate to the file.
4. Click **Open > Next**.
5. Review the entries.

   The first 15 records are displayed. Use this display to ensure you have formatted the entries correctly.
6. Click **Next**.

   The Delinea Directory - Bulk Import Report field is automatically populated with your email address. Change the address if you want the email address to go to someone else.
7. Click **Confirm**

After the wizard completes the import, the Privileged Access Service sends two email messages:

- A Delinea Directory - Bulk Import Report. This email message is sent to the email account that you had specified to receive the report. It indicates how many new users were specified in the file and how many were successfully added. An explanation is provided for each failed account.
- A Delinea Directory - New User Account. This email message is sent to each user account created. The message includes a link to the Admin Portal and a one-time password. When users open the link, they are prompted to create a new password (unless you have configured otherwise).

Note: You can customize this letter–see "How to Customize Email Message Contents" on page 251

Importing Bulk Unix Profiles

You can create or update Unix profiles for Delinea PAS users by doing a bulk import of Unix profiles. This way, you can set up the Unix profiles with UIDs and GIDs as you prefer.

You can download an import template CSV file that shows which fields you need to specify for each user or group account. This file is available from the first page of the import wizard.

Here are some important things to know:

- For each user profile you specify in the CSV file, you must at least specify the `UID`, `UnixName`, and `UPN`.
- For each group profile that you specify in the CSV file, you must at least specify the `GID`, and `GroupName`.
- When specifying new `UID` or `GID` values, it is not recommended to use 0 through 999; these UID/GID values may collide with system accounts.
- For users with existing Unix profiles, after you change their profile information, they will lose access to their current/previous home directory because of the `UID` change.
- After the import completes, you will receive a report with the import details. This report includes information about which accounts were successfully imported and any errors.
- If desired, you can use the following APIs to retrieve and set the user or group profile information. More information about these APIs are at theDelinea Developer Portal.
  - `UnixProfile/GetUserProfile`
  - `UnixProfile/SetUserProfile`
  - `UnixProfile/GetGroupProfile`
  - `UnixProfile/SetGroupProfile`

To bulk import Unix profiles and create or update Delinea PAS accounts for the profiles:

1. Go to **Access** > **Users**, and click **Import Unix Profiles**.

   The Import Unix Profiles wizard opens.
2. Click **Browse** to locate and select the CSV file that contains the Unix profile information.

   Click **Next** to continue.
3. Review a sampling of what the import wizard has brought in from your CSV file. The wizard displays a preview of the first 15 rows from the CSV file.
4. If the information is correct, click **Next** to continue.
5. Enter an email address. The service will send the Bulk Unix profile import summary to the email address you specify here.

   After the import completes, the service emails you a report summary with the import details attached in a CSV file . If the import skipped any profilesbecause of errors, the report lists them and you can review the details in the CSV file.
6. Click **Confirm** to continue.

   The wizard closes and you should see the report summary in your email inbox shortly.

Assigning Users to Roles

Before you can add Active Directory users and groups to roles, you must first integrate Active Directory with Privileged Access Service. Installing the Delinea Connector initiates the integration. See How to install a Delinea Connector. After you install the Delinea Connector, you can add those domain users to specific roles.

If you assign users to custom roles or change the default behavior for the Everybody role, it is important to verify that users can access the Privileged Access Service Admin Portal. Access to the portal is required to open assigned applications and register mobile devices.

Only members of the System Administrator role or members of a role with the Role Management administrative right can create and assign users to roles.

To Assign Users to a Role:

1. In Admin Portal, click **Roles**.
2. Select the role from the list of roles available.
3. Click **Members**, then click **Add** to display the Add Members dialog box.
4. Start typing the user name, Active Directory/LDAP group name, or an existing role.

   Entries matching the string you type are displayed.
5. Select the check box associated with the user, group, or role you want to add, then click **Add**.

   You must select a universal or security group. Local or distribution groups are not supported.

   If you are using Active Directory/LDAP as an identity store, all of the matching users accounts and groups in the Users container in the domainsthat the can “see” in the domain or forest are displayed. See Supportinguser authentication for multiple domains for more information on which domains can be “seen.”

   After you add an Active Directory/LDAP user or group to a role, the name is not shown on the Users page until the user logs in to the Admin Portal or registers a device.
6. Click **Administrative Rights** > **Add**.
7. Click **Save**.
8. Select the check box associated with the rights you want to assign.

   See "Admin Portal Administrative Rights" on page 277 for information on the rights.
9. Click **Add**.
10. Click **Assigned Applications** > **Add**.

    The Add Applications page shows the applications you have added to your tenant. See Applications for application-specific configuration instructions.
11. Select the check box associated with applications you want to assign.
12. Click **Add** > **Save**.
13. Select the check box associated with the rights you want to assign.

    See "Admin Portal Administrative Rights" on page 277 for information on the rights.
14. Click **Add**.

15. Click **Assigned Applications** > **Add**.

    The Add Applications page shows the applications you have added to your tenant. See Applications for application-specific configuration instructions.

16. Select the check box associated with applications you want to assign.
17. Click **Add** > **Save**.

Nesting a Role

You can add a Privileged Access Service role to a role. This is referred to as “nesting a role.” When you add a role to a role, the nested role members get all of the applications and rights assigned in the parent role. However, the applications and rights inherited from the parent are *not* displayed when you select the nested role. Only the nested role members have use of the rights and applications assigned to the nested role—the parent role members do not.

Additionally, if you are also using Active Directory/LDAP as an ID repository, a role can contain Active Directory/LDAP user accounts and groups.

How to Update User Account Information

Where you update user account information depends on the account source.

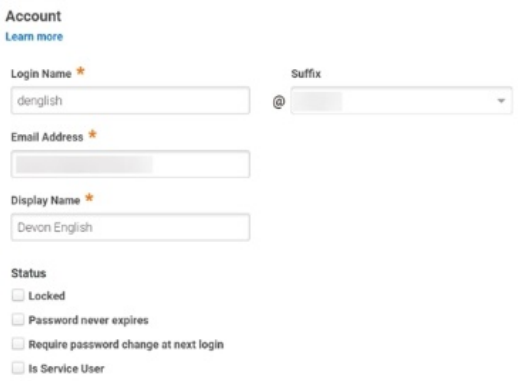
For Active Directory accounts, you must use Active Directory Users and Computers to update the account information. The update information is updated in Privileged Access Service according to the Active Directory user verification interval you set in the connector.

For other LDAP services and G-Suite accounts, you must use the relevant tool or GUI to update the account information.

For Delinea Directory accounts, you use Admin Portal to update the account information.You must be a member of the sysadmin role or any Privileged Access Service role that has the User Management administrative right to create, delete, and modify Delinea Directory accounts.

To update user information for Delinea Directory accounts

1. Log in to Admin Portal
2. Click **Users > relevant user**.



3. Update the information on the **Account** page as needed.

   Refer to the following table for more information about the fields you can change.

Option	Does this
Login Name	The login name the used to log in to the tenant. Users log in with <Login Name>@<Suffix>.
Suffix	The login suffix identifies the ID repository containing the user account when the user logs in to the portals or enrolls a device. Be careful if you change the user's login suffix because this affects their role memberships and policies. See "How to Use Login Suffixes" on page 236 for more information about login suffixes.
Email Address	The email address for the user
Display Name	The name visible to users once they are logged in to the tenant.
Locked	Locks the account. Set this field to prevent the user from launching Delinea services. This setting can either be manually enabled or enabled automatically through policy. To configure the policy, navigate to **Policies** > **Policy Set** > **User Security Policies** > **Password Settings** > **Maximum consecutive bad password attempts allowed within window** and select desired attempts. The best practice is to set the policy to a level below your directory service threshold. When locked, users are prevented further access to Delinea services but are not locked out entirely in their directory service.
Password never expires	Overrides the default "Maximum password age" policy setting. Regardless of the "Maximum password age" setting, the password for this account never expires. The default maximum password age for user service accounts is 365 days. You use the Account Security Policies > Password Settings > Maximum password age policy on the Policies tab in Admin Portal to reset this value. **Note**: This setting and the "Require password change at next login" setting are interdependent. If you select one, the other is reset.
Require password change at next login (recommended)	Forces users to create a new password the next time they log in. The user is subject to any password reset policy controls and settings you have enabled (see Applications). This setting is reset as soon as the user logs in and creates a new password. **Note**: This setting and the "Password never expires" setting are interdependent. If you select one, the other is reset.
Is Service User	Select this option for users who should NOT belong to the Everybody role. For example, you might select this option for contract or temporary users. See "Predefined Roles" on page 276 for more information.
Is OAuth confidential client	Select this option for users representing web applications with the Client ID Type set to Confidential. See the developer docs for more information.

Option	Does this
Send email invite for User Profile setup	Select this option to send new users an email invite to log in to the Admin Portal.
Profile information	Updates user profile information such as Mobile Number, User Photo, an d so forth. If you have users who will be registering devices or you are using mobile devices as a form of multi-factor authentication, be sure to put the device's phone number in the Mobile Number field.
Organization	Updates the user reporting structure. Specifying a user's manager has implications for access requests. See Managing application access requests for more information.

1. Click **Save**.
2. Update information on the **Unix Profile** page as needed, and then click **Save**. For details, see "Specifying UNIX Profile Information" below.
3. Update information on the **MFA Redirection** page as needed, and then click **Save**. For details, see "How to Use MFA Redirection" on page 350.

   The other pages (Activity, Roles, Additional Attributes, and Policy Summary) are view-only.

Specifying UNIX Profile Information

Users: If the user will be accessing enrolled Linux systems (where the Delinea Client is installed), you can specify any or all of the following fields:

- `Unix name\*`
- `Uid`
- `Gid\*`
- `UPN\*`
- `Home`
- `Shell`
- `Gecos`

If you specify any Unix profile fields, you must specify Unix `name`, `Gid`, and `UPN`. For any fields that don't have a value, the service will automatically generate them for the user when the user first logs in to a Linux system.

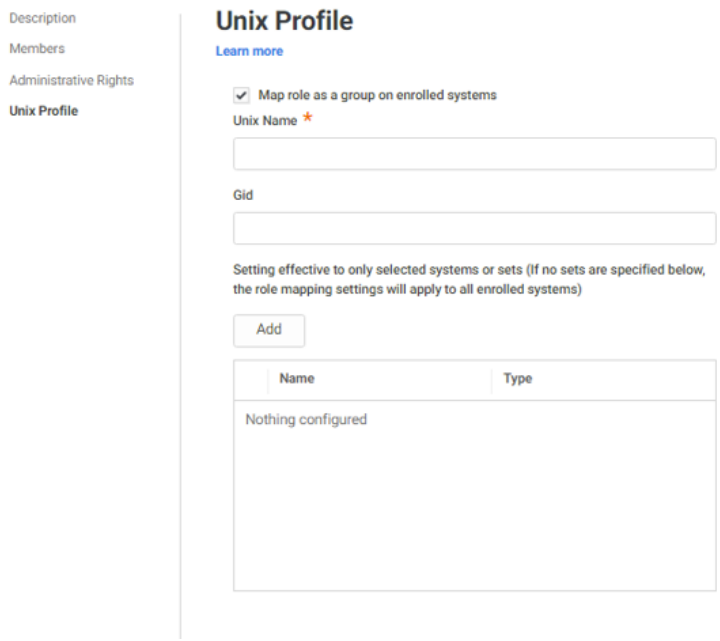
Roles: If your users assigned to the role will be accessing enrolled Linux systems, you can specify the Unix Profile information, if desired. You can map a role to either a local group that already exists on systems or a new local group. You can specify the local group by going to the **Unix Profile** page and selecting **Map role as a group on enrolled systems**.

- **Unix name**: This is the name of the new or existing local group. You must specify this field.

  Enter an existing local group name if you want to map this role to a group that exists already on your Linux systems.
- **GID**: This field is optional. If you are mapping this role to an existing local group, be sure to enter the correct GID (otherwise the mapping won't work correctly).

In the Unix profile you can specify which set(s) of systems to have your role map to.

1. Go to **Access** > **Roles** then select the role you want to map.
2. Go to **Unix Profile**.



3. Select **Add**, search for the set or sets of systems you want to map.
4. Click **Save**.

How to Push Updated Permissions to Users

If a user is affected by a change to the role's administrative rights, the change does not take affect until the user logs in again. If the user is logged in when you make the change, the pre-existing rights persist.

Use the following procedure to push the updated user's rights immediately.

To push a user's administrative rights immediately:

1. Log in to Admin Portal
2. Click **Users**.
3. Select all of the relevant users.
4. Click **Reload** from the Actions drop-down list.

How to Delete User Accounts

For Delinea Directory accounts, deleting the account means that it is disabled and no one can log in using those account credentials. For Active Directory/LDAP user accounts, deleting them from the Admin Portal only removes them from the Users page. People can still use those account credentials to log in to Privileged Access Service. You must use Active Directory Users and Computers to truly disable the account.

To delete multiple users with one command:

1. Log in to Admin Portal.
2. Click **Access > Users**.
3. Select the relevant accounts.
4. Click **Delete** from the Actions menu.
5. Click **Yes** to confirm.

Deleting Active Directory/LDAP User Accounts

Active Directory/LDAP user accounts should be deleted from Admin Portal and Active Directdory/LDAP to avoid confusion.

When you delete Active Directory/LDAP user accounts Admin Portal, the account records are deleted from Privileged Access Service, but they are unchanged in Active Directory. These users can still log in to Privileged Access Service using the same Active Directory/LDAP accounts.

When you delete Active Directory/LDAP user accounts in Active Directory/LDAP, those user accounts remain on the Users page in Admin Portal but they can no longer access Delinea Connector. For the connector to detect a user account deletion performed in Active Directory and update the Users page in Admin Portal, each Delinea Connector must have permission to read the deleted objects container in Active Directory. You can provide the necessary permission by running the following commands on each connector.

- If you do not have the necessary permissions to change the permissions of the deleted objects container, then run this command:

  ```
  dsacls "CN=Deleted Objects,DC=\<EXAMPLE\>,DC=\<COM\>" /takeownership
  ```

- The following command grants the Delinea Connector permission to read the deleted objects container in Active Directory:

  ```
  dsacls "CN=Deleted Objects,DC=\<EXAMPLE\>,DC=\<COM\>" /user:administrator@\<EXAMPLE.COM\>
  /passwd:\* /g \<EXAMPLE\>\\\<MACHINENAME\>\$:LCRP /I:T
  ```

- Deleting an LDAP Directory Service invalidates all of the users associated with that LDAP. You can not repair this by creating a new LDAP DirectoryService with the same connection parameters, as the new Directory Servicewill be considered a different Directory Service regardless of theconnection parameters. All user-specific elements must be re-created -- thisincludes OATH tokens, user security questions, role memberships - among other things.
- If an LDAP Directory Service is deleted, the users associated with that Directory Service are not automatically removed. They must be removed manually from the Admin Portal.

How to Delete a Role

You can delete any role you created. You cannot delete the sysadmin and Everybody roles.

To delete Privileged Access Service roles:

1. Log in to Admin Portal.
2. Click **Roles**.
3. Select one or more roles.

   The Add Role button is replaced by an **Actions** button.
4. From the Actions drop-down menu, click **Delete**.
5. Click **Yes** to confirm the deletion.

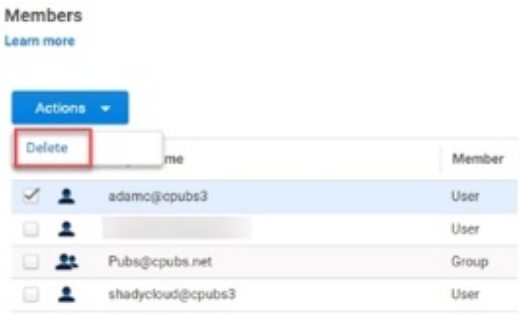
How to Remove Users or Groups from Role

When you remove users or Active Directory/LDAP groups from a role, any administrative rights or applications assigned to that role will no longer apply to those users. For example, if you have assigned the Box application to that role ABC, then users removed from that role will no longer have SSO access to Box.

To remove a role member:

1. In Admin Portal, click **Access** > **Roles**.
2. Click the role.
3. Click **Members**.
4. Click the check box for each member you want to remove.

   The Add button is replaced by an **Actions** button.



5. From the **Actions** drop-down menu, click **Delete**.
6. Click **Save**.

How to Add and Define User Attributes

In addition to the default user attributes, you can add custom ones and define the values for each user. The attributes can then be used to specify application access in the following ways:

- Define application login authentication rules (through scripting only).
- Make attributes available to the application service provider (SP) for SAML user authentication (via scripting only).

You can add and define attributes for Active Directory/LDAP and Delinea Directory users. The additional attributes are stored in Privileged Access Service only and not copied to Active Directory/LDAP. You must make all updates using the Admin Portal.

Important: You can add a maximum of 10 attributes.

Add User Attributes

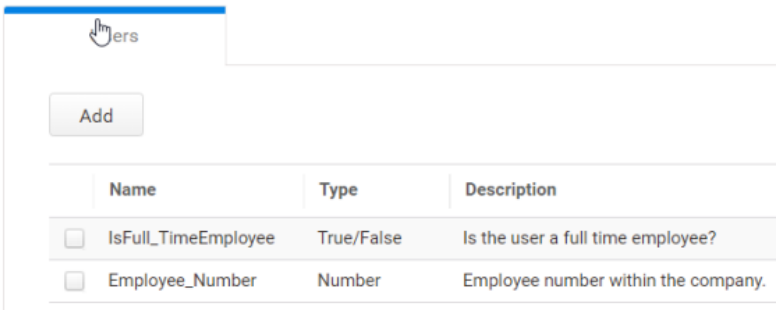
To make attributes available for login authentication rules and SAML user authentication, you must first add them to the user table. You can add a maximum of 10 attributes.

1. Log in to Admin Portal
2. Click **Settings > Users > Additional Attributes**.

   The Additional Attributes page opens.
3. Click **Users** tab > **Add** button.
4. Enter a **Name** for the attribute.

   Important: The name must contain an underscore. For example, employee_status.
5. Select the attribute **Type** from the drop-down list.
   - `Number` allows whole numbers.
   - `Number (decimal)` allows numbers with decimals.
   - `Text` allows any string.
   - `True/False` results in a drop-down list for the attribute Value.
   - `DateTime` results in a date and time picker for the attribute Value.
6. (Optional) Enter a **Description** for the attribute.
7. Click **Add**.

   The new attribute displays on the Additional Attributes page.



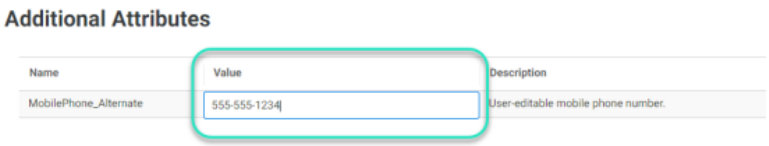
Define Attributes

You must define the attribute values for the relevant users before they can be authenticated using those attributes.

1. Log in to Admin Portal.
2. Click **Access > Users**.
3. Select the relevant user account.
4. Click **Additional Attributes**.

   You should see the custom attributes you added.
5. Click the **Value** column associated with the attribute name that you want to define.
6. Enter free-form characters or select from the drop-down list depending on the value type, then press **Enter**.

   For example, a boolean (`True`/`False`) attribute type will have a drop-down list, while a Text attribute type allows any string.



How to Use Login Suffixes

The login suffix is that part of the login name that follows @. For example, if the login name is bob.jones@acme.com, the login suffix is “acme.com.” The login suffix identifies the ID repository containing the user account when the user logs in to the portals or registers a device. If the login suffix is not listed on this page, the user cannot be authenticated.

Privileged Access Service automatically creates a default login suffix for your organization based on the login suffix in the work email account entered in the Delinea sign-up form. However, if that login suffix is already in use, the Privileged Access Service appends a one- or two-digit number to the end. For example, if the email address entered when the Privileged Access Service account had the login suffix acme.com but “acme.com” was already used by another organization, the Privileged Access Service would create the login suffix acme.com.4.

You can create more login suffixes for Delinea Directory accounts. You assign a new Privileged Access Service to a login suffix when you create the account.

Delinea Directory Specific Information

For Delinea Directory users, the customer ID in the URL can be an ID or a login suffix.

However, if you use a login suffix and the user name that is specified is a short name (without a login suffix), then the customer ID in the URL must be a login suffix. The login suffix should not look like an ID.

The following are examples of using a short name (without login suffix) user name to log in to Privileged Access Service.

URL	User name without login suffix	Restrictions
`https://companyXYZ/home?customerid=myorg.com`	jane	You must have a user account jane@myorg.com.
`https://cloud.centrify.com/home?customerId=myorg`	jane	You must have a user account jane@myorg
`https://cloud.centrify.com/home?customerId=AAA0001`	jane	Even though AAA0001 is a valid login suffix, this log in fails because the customer ID in the URL looks like a ID. For this log in to succeed, the user name should have a login suffix (for example jane@AAA0001).

Active Directory Specific Information

If you are using an Active Directory domain as an ID repository, the Privileged Access Service adds the following login suffixes when the connector is installed:

- The login suffix in the installer account name. This allows the administrator to log in to Admin Portal right after installing the connector.

  If the login suffix in the connector installer's account is already in use in Privileged Access Service, an error message is displayed and you cannotuse that domain name as a login suffix. (This occurs rarely but can happen.) Contact support if this happens to your account.
- The domain name of the domain controller to which the host computer for the connector is joined.
- If that domain controller is part of a tree or forest, the Privileged Access Service adds a login suffix for all other domains in the tree or forest it can locate.

  If you have users with Active Directory accounts in domains in a tree or forest that was not found or users who log in with their Office 365 account,you must add those login suffixes before these users can log in to Admin Portal and register a device.

  You can also create an alias for an Active Directory domain name. You would use an alias to simplify login for users with a long or complicated Active Directory login suffix. See "Creating an Alias for Long Active Directory Domain Names" on the next page for further detail. You cannot create an alias for Delinea Directory login suffixes.

Creating a Login Suffix

You can create as many login suffixes as you want for Delinea Directory accounts. The login suffix can be composed of any of the UTF8 alphanumeric characters plus the symbols + (plus), - (dash), _ (underscore), and .

(period). You can, but are not bound to, use the form label.label for your login suffixes; however, a login suffix can be composed of a single label—for example, ABCCorp.

Login suffixes must be unique in Privileged Access Service (not just within your Privileged Access Service account). If you enter a login suffix that is already in use, you get an error message.

You can select any login suffix when you create new Privileged Access Service accounts.

To create a login suffix:

1. Log in to Admin Portal and click **Settings > General > Suffix > Add**.
2. Enter the suffix in the text box and click **Save**.

Deleting a Login Suffix

You cannot delete a login suffix that has any user accounts. Admin Portal displays an error message if you try to delete a login suffix that still has user accounts. To delete a login suffix, remove all of its user accounts.

If you need to use an existing login suffix for another tenant, you will need to rename it. See "Modifying a Login Suffix" below.

Modifying a Login Suffix

You can rename a login suffix. If you do, the accounts associated with the original login suffix are automatically updated to the new one. Be sure to notify the users affected that they have a new login suffix. They will not be able to log in using the original suffix.

To modify a login suffix:

1. Open Admin Portal and click **Settings > General > Suffix**.
2. Right-click the login suffix and click **Modify**.
3. Make your changes in the text box and click **Save**.

Creating an Alias for Long Active Directory Domain Names

Best practice dictates that you use a login suffix for Active Directory users that they are already using. For example, if they're using your organization's domain name to open their email account, it would help them remember their Privileged Access Service user name if you used the same login suffix.

However, this is not a requirement. For example, if you have a long or complex Active Directory domain name, you can create a mapped login suffix for Active Directory accounts using the **Advanced** option. For example, if your login suffix is abc.bigcorp.com, you could define another login suffix, such as "abc."

To map an Active Directory login suffix:

1. Open Admin Portal and click **Settings** > **General** > **Suffix** > **Add**.
2. Enter the alias in the **Login suffix** text box.
3. Expand **Advanced**.
4. Reset the **Keep Login Suffix and Mapped Suffix the same** checkbox.

5. Backspace over the login suffix in the text box below the checkbox and enter the Active Directory domain name.
6. Click **Save**.

How to Specify User Password Complexity Requirements

You can specify the complexity requirements users must meet when creating their user passwords. If you do not make any changes, the default requirements are enforced.

To specify the user password requirements:

1. Log in to Admin Portal.
2. Click **Access** > **Policies**.
3. Select the relevant policy set or create a new one.
4. Click **User Security Policies > Password Settings**.
5. Specify the following user password requirements. Explanations for each option are available in the associated UI help.
   - Minimum password length (default 8)
   - Maximum password age (default 365 days)

     Users must have the “Enable users to change their passwords” policy (on the same UI page) set to Yes to reset their password (policy is set to Yes by default).

     If you have multifactor authentication enabled, users are prompted to create new passwords after they have fulfilled the multifactor authentication method.

     Enter 0 (zero) if you do not want to specify a password expiration period.
   - Password history (default 3)

     Enter 0 (zero) to let user use the same password.
   - Require at least one digit (default Yes)
   - Require at least one upper case and one lower case letter (default Yes)
   - Require at least one symbol (default No)
   - Show password complexity requirements when entering a new password (default No)

     The password complexity explanation/text string shown to Delinea Directory users is automatically discovered. For Active Directory, LDAP,and Google directory users, you must manually enter the explanation/text string in the associated text box.
6. Click **Save**.

How to Specify User Password Rules and Constraints

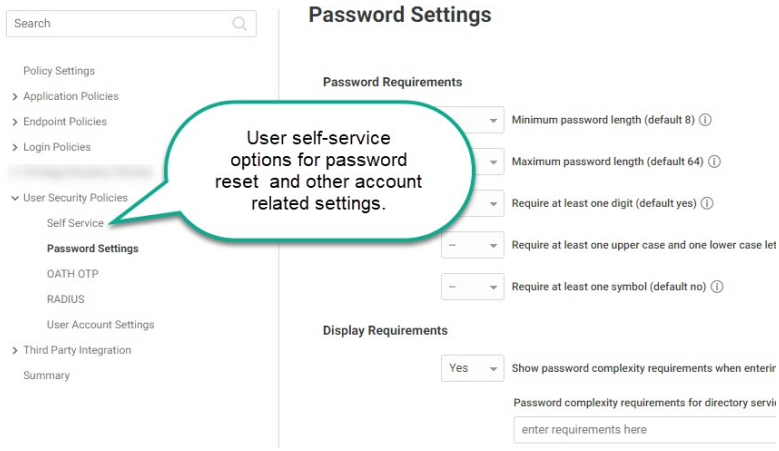
You can specify user password expiration rules and other related constraints. One rule may rely on another rule, so read the associated UI help text thoroughly. Hover your mouse over the associated “i” for the help text information.

If you do not make any configuration changes, the default rules are enforced.

To specify user password rules and constraints:

1. Log in to Admin Portal.
2. Click **Access > Policies**.
3. Select the relevant policy set or create a new one.
4. Click **User Security Policies > Password Settings**.
5. Specify the user password related rules and constraints in the Password Requirements, Display Requirements, Additional Requirements, Password Age,and Capture Settings areas. Explanations for each option are available in the associated UI help.

   It is also useful to review the user self-service options. See "Configure Password Reset Self-Service Options" on the next page



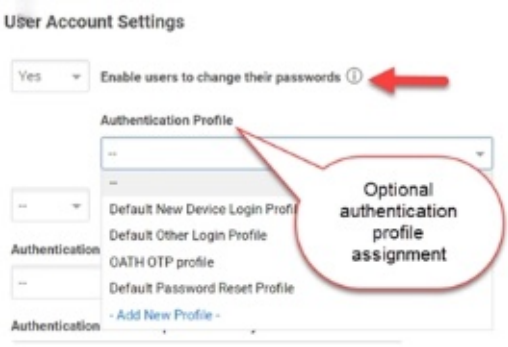
6. Click **Save**.

Configuring user password change options

This user password change option is independent of those available in **User Security Policies > Self Service > Password Reset**.

To configure user password change options:

1. Log in to Admin Portal.
2. Click **Access** > **Policies**.
3. Select the relevant policy set or create a new one.
4. Click **User Security Policies > User Account Settings**.
5. Select **Yes** in the **Enable user to change their passwords** drop-down list.



If this policy is set to No and you use the **Maximum password age** policy to set an expiration date for the password, users will not be able to reset their password. Instead, an administrator will have to reset the password for them.

6. (Optional) Select from the **Authentication Profile** drop-down list to specify the authentication mechanism users must provide to change their password.

   See "Creating Authentication Profiles" on page 284 for authentication profile information.

7. Click **Save**.

How to Configure User Self-Service Options

You can enable users to perform certain tasks related to their accounts. These tasks include password reset and account unlock options. If you want to enable these features for Active Directory users, you need to run the Delinea Connector under an account with the necessary permissions and follow these procedures.

This scenario includes the following topics:

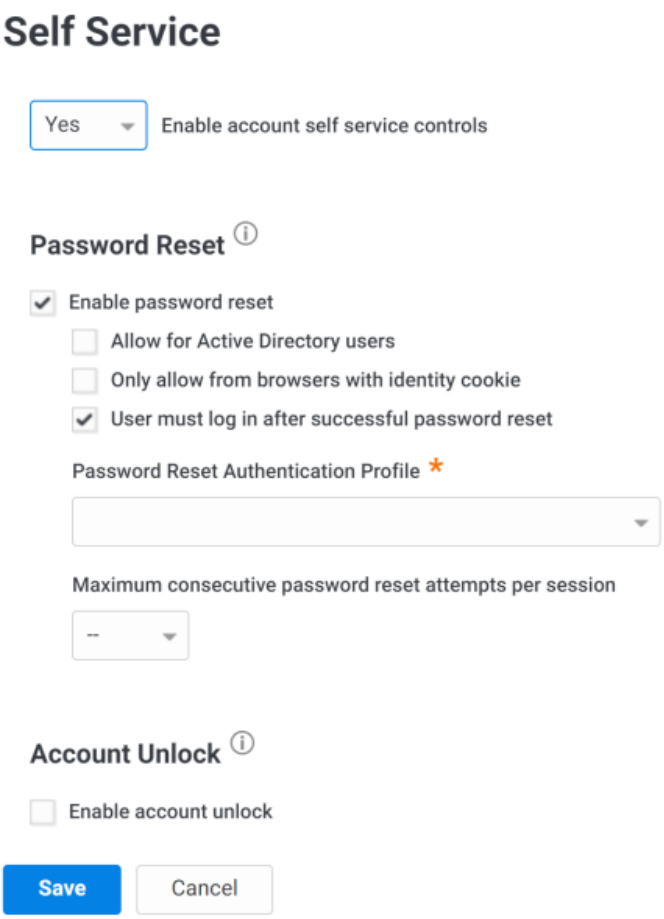
- "Configure Password Reset Self-Service Options" below
- "Configure Account Unlock Self-Service Options" on page 246

Configure Password Reset Self-Service Options

You can enable users to reset their passwords and specify additional authentication requirements for a password reset.

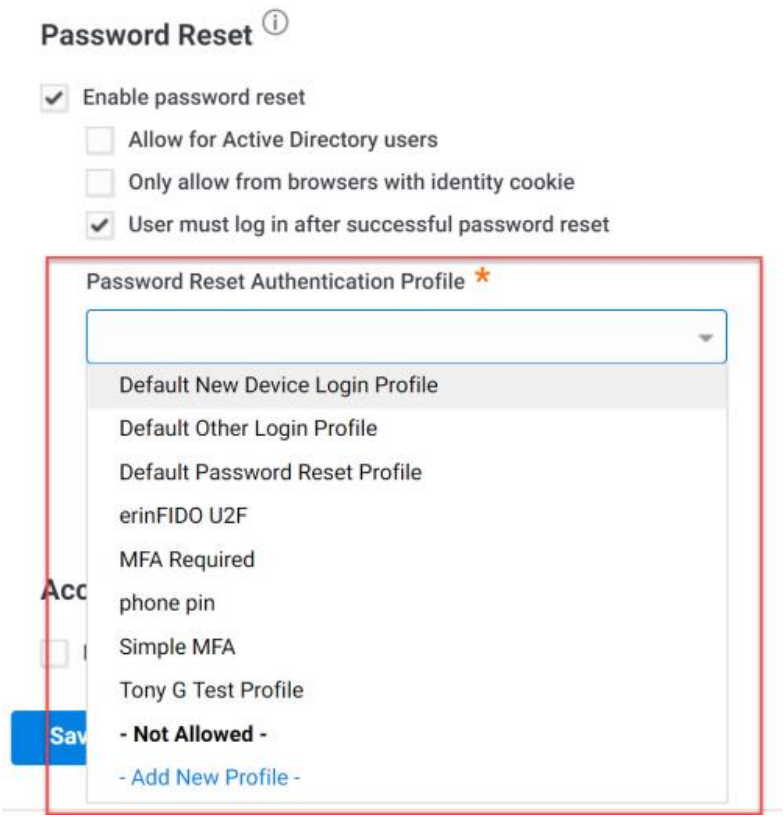
To Enable the Password Reset Self-Service Options

1. Log in to Admin Portal, click **Access** > **Policies** tab, and select the policy set.
2. Click **User Security Policies > Self Service**.
3. Select **Yes** in the Enable account self service controls drop-down.
4. Enable the **Password Reset** option.



5. Limit who can reset their passwords.
   - The “Allow for Active Directory users” option enables users with Active Directory accounts who have forgotten their password to log in and reset their password. If you do not set this option, the “Forgot your password?” link is not displayed in the login prompt for users with Active Directory accounts. If you set this option, then you need to configure the **Active Directory Self Service Settings** on this page.
   - The “Only allow from browsers with identity cookie” option restricts password reset to those users who have already logged in successfully. If this check box is not enabled, then anybody can use the password reset options.

     The Privileged Access Service writes the identity cookie the first time the user logs in successfully. However, when users clear the history on their browsers, it removes this cookie.
   - The “User must log in after successful password reset" option requires the user to log in after a password reset.
6. Select the authentication profile to specify the authentication mechanisms/second-factor authentication users must provide before they can reset their passwords.



You can use a default profile, use an existing profile, or create a new one.

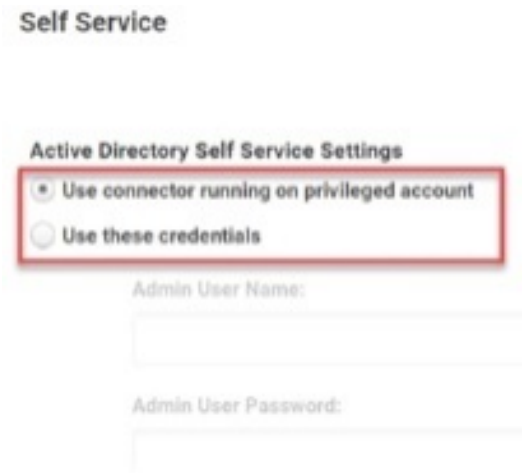
See "Creating Authentication Profiles" on page 284 for more information.

Note: Self-service password reset is unavailable inside the MFA grace period.

For more information about setting the MFA grace period for Windows or Mac, see or , respectively.

7. Configure options for enabling password reset for Active Directory users.

   This option is only available if you have enabled the “Allow for Active Directory users” option.



- Select **Use connector running on privileged account** to run the connector under an account that has the Reset Password permission. Unless you have changed the connector account after you ran the connector installation wizard, the connector is run as a Local System account process. By default, a Local System account does not have the Reset Password permission. See "Permissions Required for Alternate Accounts and Organizational Units" on page 412to set the permission.

  Optionally, after you select this **Use connector running on privileged account** setting, you can assign password reset permission for Active Directory users by creating a security group in Active Directory, delegate that group the Reset Password permission (see Password Reset Permissions), and add the connector's computer object(s) to that group.
- Select **Use these credentials** to use an account with the required permission to reset the password. For example, any account in the connector's Domain Admins group can reset another user's Active Directory account password.

8. Set the additional policy parameters.

   The additional policy parameters let you manage the following password reset behaviors:

   - Maximum forgotten password resets allowed within window

     Use the drop-down list to set a maximum for the number of times users can reset their password within the capture window. If users exceed this limit, the next time they attempt to reset the password, they get a message that they have reset their password too often and must wait before attempting again.
   - Capture window for forgotten password resets

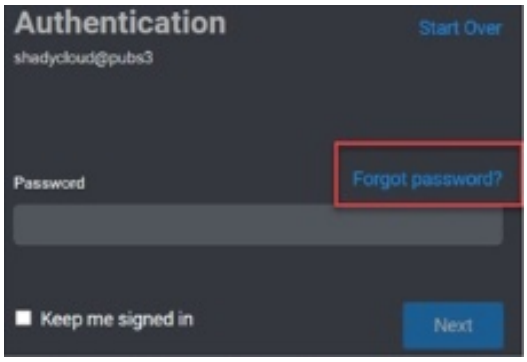
     Use the drop-down list to set the time period for maximum forgotten password resets. When users exceed the number or resets in this time period, they cannot reset the password again. This value also specifies how long from the last reset attempt the user must wait before they are allowed to reset the password.
9. Specify the **Maximum consecutive password reset attempts per session** option.

   This option specifies the number of attempts users have to reset their password for that session before they are taken back to the log-in page. The default is 5 attempts.
10. Click **Save**.

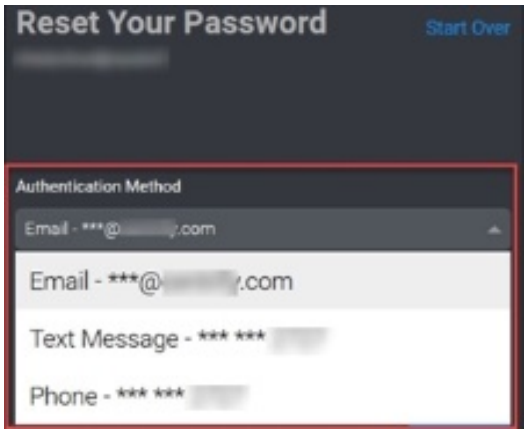
What Your Users See

After you enable this policy setting and push the policy, users can do the following

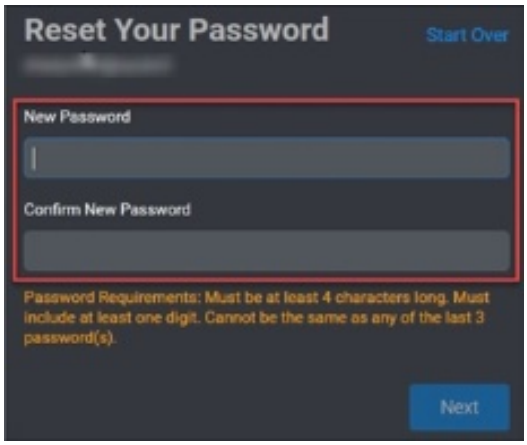
1. Click the **Forgot password?** link from the Privileged Access Service login window.



   The authentication mechanisms you specified in the authentication profile (step 6 above) are shown to users as options for confirming their identities before they can reset their passwords.



2. Select the authentication mechanism you want to use.
3. Click **Next**.
4. Satisfy the selected authentication mechanism.
5. Enter your new password.



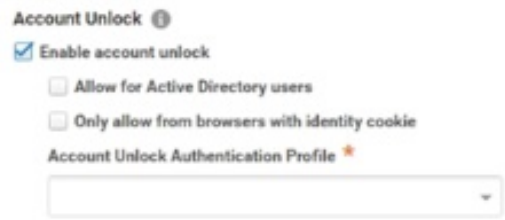
6. Click **Next**.

Configure Account Unlock Self-Service Options

You can enable users to unlock their accounts.

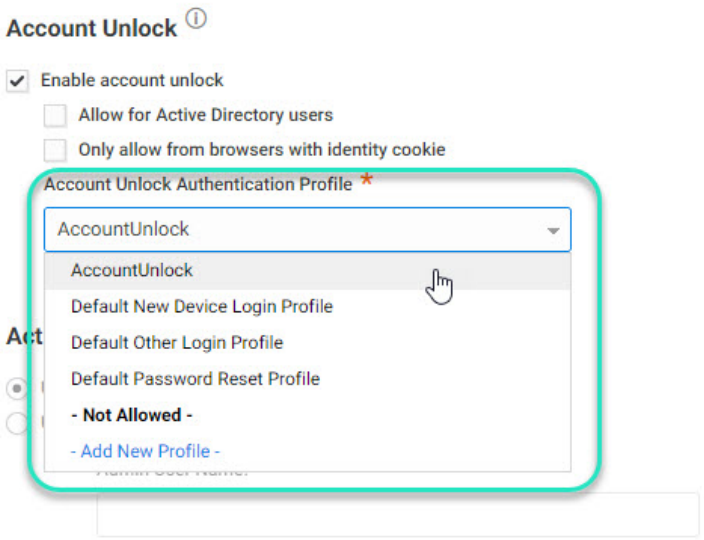
To enable account unlock policies:

1. Log in to Admin Portal, click **Access** > **Policies** tab, and select the policy set.
2. Click **User Security Policies > Self Service**.
3. Select **Yes** in the Enable account self service controls drop-down.
4. Enable the **Account Unlock** option.



5. Limit who can unlock their accounts.
   - The “Allow for Active Directory users” option enables users with Active Directory accounts to unlock their accounts. If you do not set this option, the “Unlock your account?” link is not displayed in the login prompt for users with Active Directory accounts. If you set this option, then you will need to configure the **Active Directory Self Service Settings**.
   - The “Only allow from browsers with identity cookie” option restricts account unlock to those users who have already logged in successfully. If this box is not set, anybody can use the account unlock option.

     The Privileged Access Service writes the identity cookie the first time the user logs in successfully. However, when users clear the history on their browsers, it removes this cookie.
6. Select the authentication profile to specify the authentication mechanism/second-factor authentication users must provide before they can unlock their accounts.



You can use a default profile, use an existing profile, or create a new one. Users can't use the same factors to unlock the account that they use to login, so make sure the authentication profile used for account unlock has additional factors selected and the user account has the necessary attributes to use them.

For example, if the user typically logs in with the "Password" and "Email confirmation code" challenges, you could select the "Text message (SMS)confirmation code" challenge in the authentication profile used for self-service account unlock. To pass an SMS challenge, the user account must have a valid value for the "Mobile Number" attribute.

See "Creating Authentication Profiles" on page 284 for more information.

7. Configure options for enabling account unlocking for Active Directory users.
   - Select **Use connector running on privileged account** to run the connector under an account that has the User Account Control permission. Unless you have changed the connector account after you ran the connector installation wizard, the connector is run as a Local System account process. By default, a Local System account does not have the User Account Control permission. See "Permissions Required for Alternate Accounts and Organizational Units" on page 412 to set the permission.

     Optionally, after you select this **Use connector running on privileged account** setting, you can assign account unlock permission for Active Directory users by creating a security group in Active Directory, give a user or group permission to read and write the Lockout Time attribute for an OU or other container, and add the connector's computer object(s) to that group.

   Select **Use these credentials** and provide the account user name and password to use an account with the required permission to unlock the account. For example, any account in the connector's Domain Admins group can unlock another user's Active Directory account.
8. Click **Save**.

How to Configure Idle Session Timeout

You can automatically log out users from Admin Portal after a period of inactivity. The default inactive period is five minutes.

This policy has no effect on mobile device users.

To Enable Automatic User Log Out:

1. Log in to Admin Portal.
2. Click **Settings > Users > Idle User Session Timeout**.
3. Select **Automatically log out idle users**.
4. Enter the time period.
5. Click **Save**.

How to Update the Default Administrator Account

Privileged Access Service creates a default Delinea Directory administrator account when your organization signed up. The login name of the default account is based on the work email account entered in the Privileged Access Service sign-up form. Typically, the login name to the default Privileged Access Service account uses the following format: "admin_<username>@<emailsuffix>" (where username@emailsuffix is the email address of the account used to register for the service). For example, if the email account is bob.smith@acme.com, the default Privileged Access Service account is admin_bob.smith@acme.com. Legacy tenants may likely use a default admin name of cloudadmin@<emailsuffix>.

If the email suffix in the email account is already in use by another Privileged Access Service customer, a number is appended to the login suffix. The login suffix is that part of the full account name following “@” -- “acme.com” in this example. For example, if “acme.com” is already in use, the default Privileged Access Service administrator account would be bob.smith@acme.com.2 (or another number).

The account name is provided in the email you received after you signed up. You use this account to log in to Privileged Access Service. This account is automatically added to the sysadmin role, giving you full administrator permissions in the Privileged Access Service.

Updating the default administrator account is the same as updating any account. You typically update this default account because the person who registered the tenant has left your organization. It is important to ensure the default administrator account name has a unique value and does not match any Active Directory or LDAP user account. This account is critical for troubleshooting when Active Directory login is unavailable. You can use an email address for the account that does match a local directory user.

For account recovery purposes, we recommend that you keep the account username and password in a safe location and to ensure account self-service options for password recovery are enabled. See "How to Configure User Self-Service Options" on page 241.

To update the default administrator account:

1. Log in to Admin Portal.
2. Click **Users** and select the default user account.
3. Update the relevant fields, for example the email address and login name.

   The email address of the account can be used for account recovery and to satisfy MFA challenges.
4. Click **Save**.

For account recovery and lockout assistance when self-service options are not available, please contact Delinea Support.

How to Customize the Admin and Login Window

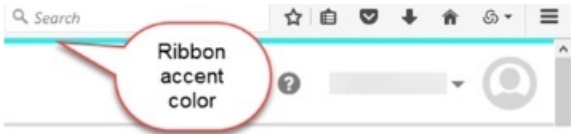
You can customize the look and feel of your Admin Portal.

You can restore the defaults for most options by clicking **Reset**.

Note: Customizations may not display with the initial user log in. Users may need to re-log in to see the changes reflected.

To Customize the Look and Feel

1. Log in to Admin Portal.
2. Click **Settings > General > Account Customization**.
3. Edit the fields under **Global Options**.
   - Enter the hexadecimal color code for **Portal Ribbon Accent Color** to change the ribbon color. Do not enter the RGB value.



   - Enter the hexadecimal color code for **Portal Ribbon Color** to change the ribbon color. Do not enter the RGB value.

   - Enter your **Company Name**.
   - Browse to and select the image file for the **Portal Image** and click **Open**.
4. Edit the fields under **Login Customization**.
   - Define the User Name hint text displayed to users on the login page window. You can click **Reset** to reset this field to its default value of user@domain.

- Click **Upload** to browse to and select the image file for the **Login Image**, then click **Open**.
- Click **Upload** to browse to and select the image file for the **Login Background Image**, then click **Open**.

  The background image must have a file size between 512 Bytes and 5 MB, with dimensions of at least 700 x 490. Support file types are .png, .jpg, .ico, .bmp, and .gif (non-animated).
- Enter the URL to your company **Terms of Use**.

  Terms of Use will appear below the login image.
- Enter the URL to your company **Privacy Policy**.

  Privacy Policy will appear below the login image.

5. Edit the fields under **Message Customization**.
   - Click **Upload** to browse to and select the image file for **Email Image**.

     This is typically your company logo, and is only used for customized messages.
   - Edit any of the default response templates provided.
     a. Click the row associated with the template.
     b. Edit the **Language**, **Email Subject**, **Display Name**, and **Email Address** fields as needed.
     c. Click the Script tab to modify the content of the message as needed. The message body can be found in the HTML on the script tab.
     d. In the Forgot User Name message template, you can change the message to drop the login suffix when the email is sent to a user by replacing the variable `{UserList}` with `{UserLoginNameList}`.

        Make the change on the Script tab, then return to the Preview tab to verify the variable has changed. The result is the user receives an email with a list of usernames matching their email address that do not include the login suffix. This can prevent confusion for users when you use multiple login suffixes.
   - Optionally, to undo customizations:

     Click the **Reset** button associated with User Name Hint Text at Login to use the default hint text.

     Click the **Reset** button at the bottom of the page to use the default settings for all the customization options on this page.

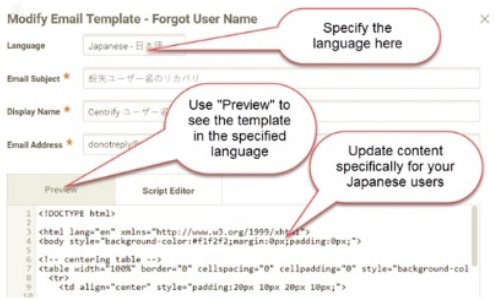
     Click the **Reset** button on the message template to use default settings for that message template.
6. Click **Save** to exit.

How to Customize Email Message Contents

Privileged Access Service use email messages to simplify log in and device registration for users, as well as for other notifications. You can upload your company logo and customize the wording and styles for these email messages.

To modify a message:

1. Log in to Admin Portal.
2. Click **Settings > General > Account Customization**.
3. Click the template you want to edit.
   - Use the Language drop down list to configure the template for the corresponding language. For example, if you have password confirmation change information that is specific to your Japanese users, you can add that information to the “Confirm Password Change” template by selecting Japanese in the drop down list.



   - Update the **Email Subject**, **Display Name**, and **Email Address** of the recipient if necessary.
   - Use the **Script Editor** to make changes to your email message.
   - Click **Preview** to see the message from the end user’s perspective.

     The following templates are available:

Template Name	Purpose
MFA Challenge	An email message sent to users when they log in to the Admin Portal. **Required**: You must enable authentication policy controls and select “Email Confirmation code” as one of the multifactor authentication options. See "How to Define Authentication Requirements" on page 280 . When users get this email, they can click “Continue with authentication” or enter the one-time passcode on the log in screen to complete the log in. Do not change `href='{AuthLink}' or {AuthCode}.`
MFA Challenge with Code	An email message sent to users when they log in to the Admin Portal. **Required**: You must enable authentication policy controls and select “Email Confirmation code” as one of the multifactor authentication options. See "How to Define Authentication Requirements" on page 280. When users get this email, they enter the one-time passcode on the log in screen to complete the log in. Do not change `{AuthCode}`.

Template Name	Purpose
Bulk User Import Report	An email message sent after a bulk register that indicates how many accounts were created out of the total requested and lists the names from the file for whom accounts could not be created (see "How to Bulk Import User Accounts" on page 224). Do not change `{CreatedUsers}, {TotalUsers}, or {FailedSummary}`.
Bulk OATH Token Import Report	An email message sent after a bulk import of OATH tokens that indicates the number of successful tokens imported out of the total and percentage of failed imports. See "How to Configure OATH OTP" on page 347 Do not change: `{TotalSuccess} {TotalRecord} {% if TotalFailed \> 0%} {% endif %} {FailedSummary}`
Bulk Corporate Owned Device Import Report	An email message sent after a bulk import of corporate owned devices that shows the number of successful devices imported out of the total and percentage of failed imports. See "How to Select the Policy Service for Device Management" on page 738. Do not change: `{TotalSuccess} {TotalRecord} {% if TotalFailed \> 0%} {% endif %} {FailedSummary}`
Invite User	Emails sent to users you selected in the Invite users procedure. Emails sent to users you selected in the Invite users procedure to simplify log in to the Admin Portal. Note: This message is sent only to users who have an Active Directory/LDAP account. This message uses the user's company account (that is, Active Directory/LDAP) credentials to authenticate the user. Do not change `href='{LoginLink}'`.
Invite User with OTP	An email sent to the users you selected in the Invite users procedure. The user can also use this message to register a device. **Note**: This message is sent only to users who have a Privileged Access Service account. This message contains the users' Privileged Access Service account name and uses it and a one-time passcode to authenticate the user. Do not change the following: `login name: {UserName} href='{LoginLink}' href='{UploadLink}'`
Forgot User Name	Email message sent to users when they initiate a password reset. The email includes a click-able user name that users can use to define a new password. Do not change `{UserList}`.
Confirm Password Change	Email message sent to users when they have changed their password.
Zone Role Assignment Request	An email message sent to users who can approve or deny a request from another user for assignment to a role on an agent-managed computer that is joined to a Delinea hierarchical zone. The email message includes a link to the request details page, from which the recipient can approve or deny the request.

Template Name	Purpose
Zone Role Assignment Approved	An email message sent to a requester upon approval for assignment to a role on an agent-managed computer that is joined to a Delinea hierarchical zone. The email message includes links to log in to the agent-managed computer, and to view request details.
Zone Role Assignment Denied	An email message sent to a requester upon denial of assignment to a role on an agent-managed computer that is joined to a Delinea hierarchical zone. The email message includes a link to view request details.
Zone Role Assignment Request Failed	An email message sent to a requester when a request for assignment to a role on an agent-managed computer that is joined to a Delinea hierarchical zone could not be processed. For example, this message is sent if an account or email address for specified approver could not be located. The email message includes a link to view request details.

1. Right-click the template and click **Reset** to restore the template to its original content.
2. Click **Upload** associated with the Email Image heading to upload your company logo for the email.
3. Click **Save**.

How to Configure Custom SMTP Server Settings

You can configure Privileged Access Service to use custom SMTP server settings for outgoing mail service such as MFA challenges and self-service features. Using custom SMTP server settings provides additional control over email behavior.

To minimize the risk of email delays, you can spread the traffic going to an ISP by whitelisting relevant IP address or hostnames. The information in the following tables may get updated over time.

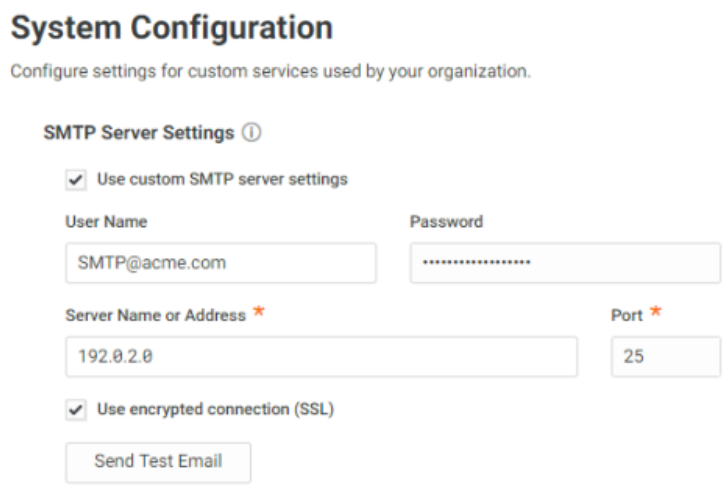
Delinea Pods

IP Address	149.72.136.199 149.72.134.160 198.37.151.203
Domain	email..centrify.com
Host	o1.email..centrify.com o3.ptr8463..centrify.com

In addition, you can use the Delinea Connector to connect to your SMTP server. This allows you to connect to the SMTP server from a known IP address if you want to limit connections based on IP address. Refer to Installing a Delinea Connector for more information about the connector.

To Configure Custom SMTP Server Settings

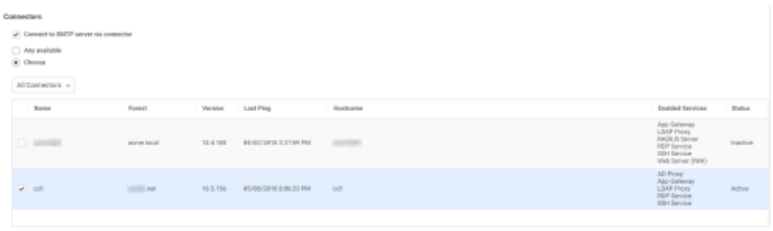
1. Login to the Admin Portal.
2. Click **Settings** > **General** > **System Configuration**, then enter appropriate credentials, server name or address, and port for your SMTP server.



3.

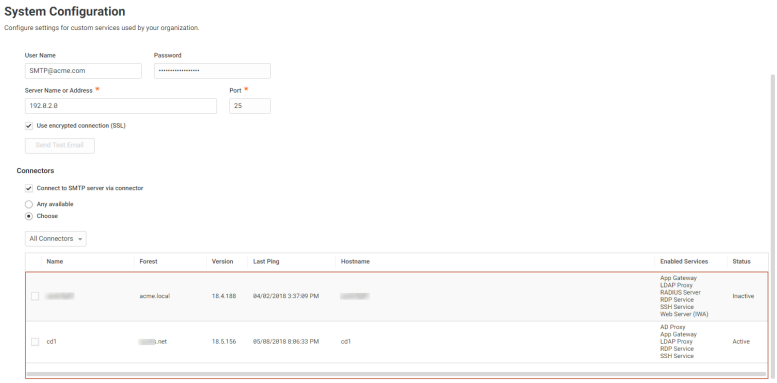
4. Select whether to use an encrypted connection (SSL).
5. (Optional) Select **Connect to SMTP server via connector**.

   This allows you to connect to the SMTP server from a known IP address if you want to limit connections based on IP address.
6. (Optional) Select either **Any available** to use any available connector, or **Choose** to select the connector that you want to use to connect to the SMTP server.



   Tip: Select a connector with a Status value of Active.
7. Update your SMTP server configuration with the IP address(es) of the selected connector(s).
8. Click **Send Test Email** to verify the custom settings.

   The Sent Test Email button is not available if you selected Connect to SMTP server via connector, but did not select a connector. For example:



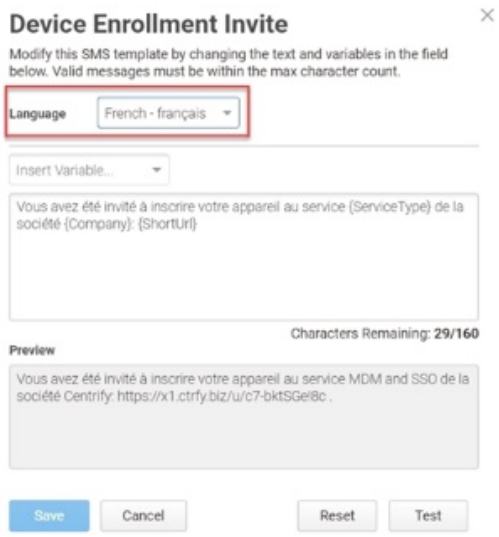
9. Click **Save**.

How to Customize SMS Message Contents

Privileged Access Service uses SMS messages to simplify device registration for users and to send MFA link and/or code. You can customize the wording for these messages.

To modify a message:

1. Log in to Admin Portal.
2. Click **Settings > General > Account Customization**.
3. Click the template you want to edit.
   - Use the **Language** drop down list to configure the template for the corresponding language.
     For example, if you have device registration information that is specific to your French users, you can add that information to the “Device Enrollment Invite” template by selecting **French** in the drop down list.



   - Click **Test** to send a test SMS message to the registered device associated with your systems administrator account.

     The following templates are available:

Template Name	Purpose
SMS MFA Challenge	A SMS message sent to users when they log in to the Admin Portal. **Required**: You must enable authentication policy controls and select “Text message (SMS) confirmation code” as one of the multifactor authentication options. See "How to Define Authentication Requirements" on page 280 . When users get this SMS message, they can click “Continue with authentication” or enter the one-time passcode on the log in screen to complete the log in. Do not change `{SmsCode}` or `{ShortUrl}`.
SMS MFA Challenge for Legacy RADIUS	A SMS message sent to users when they connect to a VPN server through Privileged Access Service (Delinea Connector as a RADIUS server). See "Configuring the Delinea Connector for Use as a RADIUS Client" on page 335**Required**: You must enable authentication policy controls and select “Text message (SMS) confirmation code” as one of the multifactor authentication options. See "How to Define Authentication Requirements" on page 280 . When users get this SMS message, they enter the one-time passcode on the log in screen to complete the log in. Do not change `{SmsCode}`.
Device Enrollment Invite	

1. Right-click the template and click **Reset** to restore the template to its original content.
2. Click **Save**.

How to Add a Directory Service

You can add LDAP or Google as directory services in the Delinea Admin Portal. If you have the same username in multiple directory services, you can set the look-up order so your preferred directory service is searched first.

Refer to the following procedures for details.

Adding LDAP as a Directory Service

LDAP communicates with the Delinea Connector over TLS/SSL on port 636. As part of the client/server handshake between the connector and the LDAP server, the LDAP server must present the connector with an X.509 certificate. To establish a trust relationship between the connector and the LDAP server, you must install the CA certificate that issued the LDAP server’s Server Authentication certificate on the machine running the Delinea Connector (specifically, the Local Computer Trusted Root Certification Authorities certificate store).

Your LDAP servers must meet the following minimum requirements before you add LDAP as a directory service.

- The server must support reading of the server's Root DSE (RFC 4512, section 5.1), and the Root DSE attributes must indicate that the server supports the LDAPv3 protocol.

  As LDAPv2 was retired in 2003, most current servers will meet this requirement; however, any server that fails to meet these requirements is not supported.
- A per-entry attribute that can be used as a server-scope unique identifier is required.

This attribute should be invariant, i.e. it should never change for the lifetime of the entry. This will default to the DN, but if the DN is liable to change in your installation you can specify a different attribute. In this case an operational attribute such as entry Uuid is preferred. If your LDAP server/schema lacks this operational attribute then you can try using a"unique" structural attribute as an alternative, but Delinea does not recommend or support this.

In either case, if the attribute ever changes then the user/group that it represents will be seen as a different user/group, resulting in orphaned users, "lost" OATH tokens, and deleted app settings and assignments. It is extremely important that care be taken to select an appropriate attribute. Information about best practices for selecting an attribute for this purpose can be found here.

Note: The selected attribute may not be changed after the configuration is created.

- An attribute containing the user's login name must exist and must be able to be queried to obtain the entity's DN, and a simple bind using that DN and a provided credential must be able to be successfully completed.
- The server must support the Modify Password Extended Operation for password reset/change to work as expected.

Delinea's LDAP support is flexible enough that some servers not meeting the minimal requirements could be configured successfully, but Delinea does not recommend or support servers that do not meet the minimal requirements.

Note: To use the Group DN feature, your connector must be using version 21.2 or greater.

To Add LDAP for the Connector

1. Log in to Admin Portal as a system administrator.
2. Click **Settings > Users > Directory Service > Add LDAP Directory**.
3. In the Settings tab, provide the required information.
   You can optionally set the **Group DN** to specify an alternate DN just for groups.

   Note: When not set, the Base DN is used for both users and groups.

4. Click the **Mappings** tab to map your LDAP instance. See "Configuring LDAP Directory Service" on the next page for details on how to map your LDAP instance.
   - For group searches, the mapping will apply the keyword search to the group name and user's display name.
   - For user searches, the mapping will apply the keyword to the user's display name, first name, last name, email, and login name.
5. Click **Connectors** and select the Delinea Connector to use with this service or let the LDAP server find an available cloud connector.
6. Click **Save**.

For additional information on configuring an LDAP service, see "Configuring LDAP Directory Service" on the next page for details.

Adding Google as a Directory Service

If you are using G Suite to store and manage your user information, you can configure Privileged Access Service to recognize it as a directory service. Users can then use their Google account details to log in to Admin Portal.

To add G Suite as a directory service

1. Log in to Admin Portal as a system administrator.
2. Click **Settings > Users > Directory Service > Add Google Directory**.
3. Click **Authorize** and enter your G Suite administrator credentials.
4. (Optional) Click **Add** to enter a redirect URI if you want your users to use a more recognizable URI that is specific to your organization.
5. Click **Save**.

Repeat the above procedure to add another Google directory.

Note: If you use Google directory for managing your users, then do not deploy the G Suite SAML application to those same users. If you do, those users will not be able to authenticate into both Google and Privileged Access Service because they will be redirected back and forth between Google directory and Privileged Access Service.

Order Directory Service Lookup

If you have the same username in multiple directory services, you can set the look-up order so your preferred directory service is searched first. For example, you might want LDAP to be searched before AD. Directory services are listed in the order of look-up. You can change the list order to your preferred look-up order.

Note: Delinea Directory is always listed first, and Federated Directory is always listed last. You can only change the order of AD, LDAP, and Google.

To change the directory look-up order

1. Click **Change Look-up Order**.
2. Drag and drop the listed directory services until they are in the preferred order.

   Directories listed on top are searched first
3. Click **Save Look-up Order**.

Configuring LDAP Directory Service

You can map, modify, test, or delete an LDAP Directory Service instance as detailed in:

- "Mapping a New LDAP Directory Service" on the next page
- "Testing the Attribute Mapping" on the next page
- "Updating an Existing LDAP Directory Service" on page 260
- "Deleting an LDAP Directory Service" on page 260

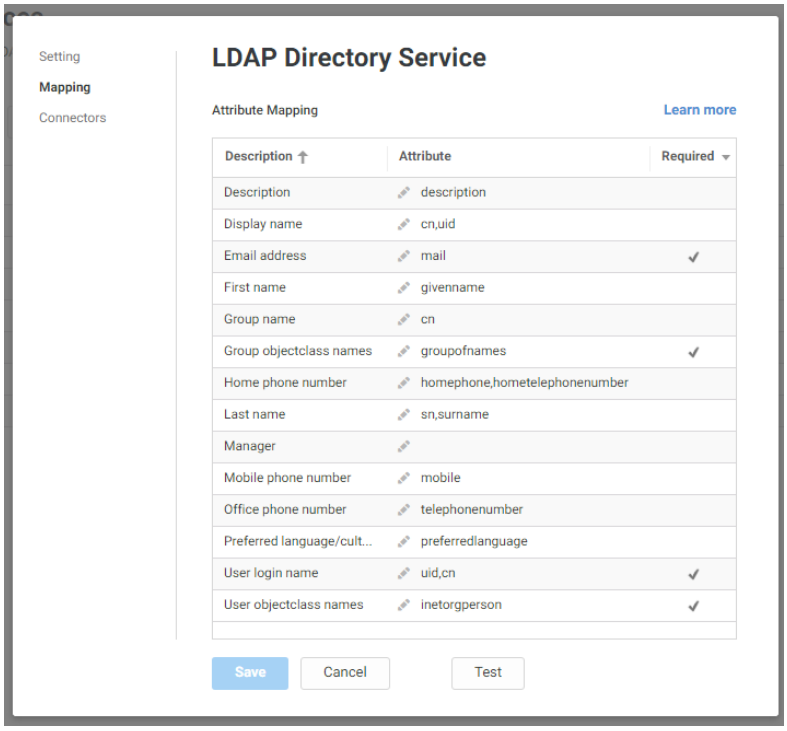
Mapping a New LDAP Directory Service

To add and map a new LDAP Directory Service instance, perform the following steps:

1. Log in to the Admin Portal as a system administrator.
2. Click **Settings** > **Users** > **DirectoryServices** > **Add LDAP Directory**.
3. Provide the required information.
4. Click the **Mappings** tab. To set up a mapping for your LDAP, edit the attribute names in the right column to the names of the attributes in your LDAP schema that fulfill the description in the left column.

   Attribute mappings may be set to required (denoted by a check in the Required column) or optional. You may choose to use several mappings simultaneously. LDAP will search for all parameters used in the mapped attributes.

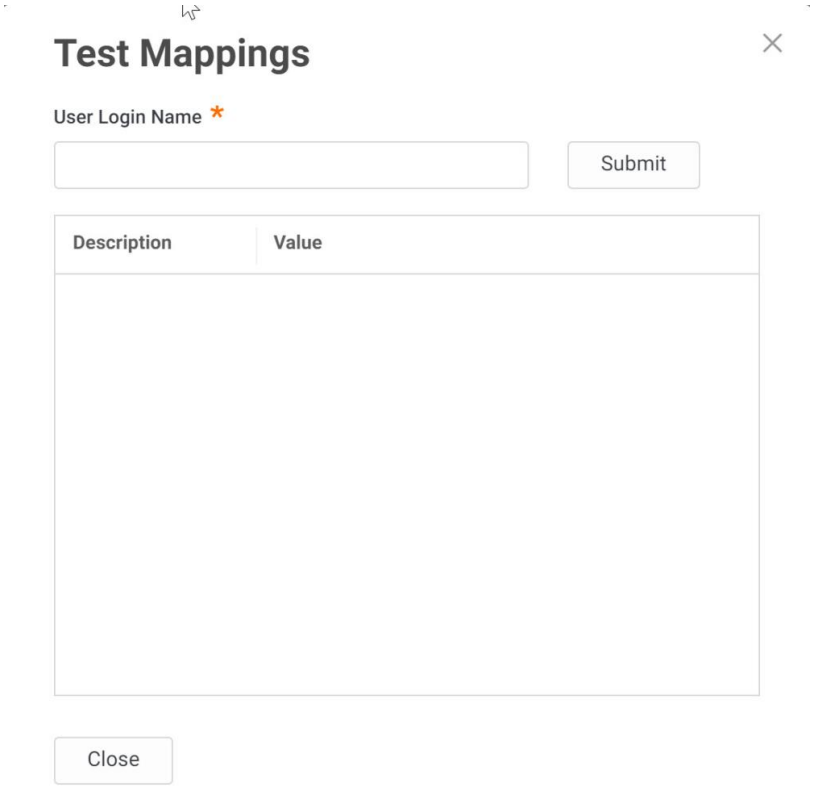
   Note: The attribute mapping for "Unique Identifier" cannot be modified after saving the configuration.



5. Click **Connectors** and select the Delinea Connector to use with this service or let the LDAP server find an available cloud connector.
6. Click **Save**.

Testing the Attribute Mapping

Once you have completed mapping the LDAP service, click the **Test** button and enter the login name of the user you wish to test. The user entry will be loaded from the LDAP server and the attribute mapping results for that user are displayed.



Updating an Existing LDAP Directory Service

To update an existing LDAP Directory Service instance, perform the following steps:

1. Log in to the Admin Portal as a system administrator.
2. Click **Settings** > **Users** > **DirectoryServices** and click an existing LDAP Directory Service instance.
3. Update the values needed and click **Save**.

Deleting an LDAP Directory Service

To delete an LDAP Directory Service, perform the following steps:

1. Log in to the Admin Portal as a system administrator.
2. Click **Settings** > **Users** > **DirectoryServices** and select an existing LDAP Directory Service account.
3. Navigate to **Actions** and choose **Delete** from the dropdown.

Troubleshooting – LDAP Server Unavailable

Issue

I'm unable to configure the LDAP server in Cloud Manager. I get the error message, "LDAP server is unavailable".

Possible Explanations

- The DNS name cannot be resolved by the Delinea Connector machine.
- There is no network route to the LDAP server from the Delinea Connector machine possible because of firewall rules or other routing issues.
- The LDAP server is not listening on port 636.

Verification Steps

Perform the following steps to verify the possible explanations:

1. From the Delinea Connector machine, confirm that the DNS name can be resolved with dns look-up.
2. If the above confirmation is successful, confirm that there is a network path to the LDAP server by telneting to it on port 636. If the screen goes blank, it means we can connect. Use **ctrl]** and type “quite” to exit.

Solutions

If the name cannot be resolved, try to enter the name in the hosts table or use the IP address of the machine. If the latter, you will likely need to un-check **Verify Server Certificate** on the **Add LDAP Directory** page.

If the server is NOT listening on port 636, append the port to the DNS hostname; for example: <dns hostname>:3269

Note: We only support LDAP over SSL. We do not support clear LDAP.

How to Set Up Business Partner Federation

Business Partner Federation establishes a trust relationship between the Service Provider (SP) and Identity Provider (IDP) using SAML tokens. By establishing this trust relationship, you can provide access to the resources that you want to share. You can federate to the following partners:

- Integrating with Microsoft Azure Active Directory
- Integrating with Idaptive tenants
- Integrating with Okta
- Integrating two Delinea tenants

There are two use cases for Business Partner Federation as follows:

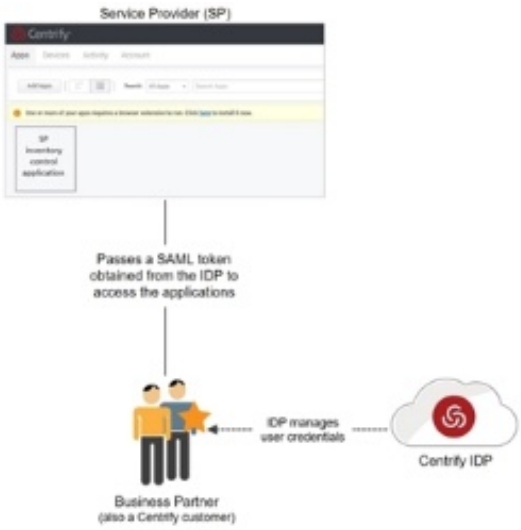
- "Shared Tenant" below
- "Tenant-to-Tenant" on the next page

Shared Tenant

In this use case, you share your Delinea tenant with your business partners. Your Delinea tenant (which hosts the services/applications) serves as the SP and your partner serves as the IDP. Your business partners access the tenant and its associated resources/applications by passing a SAML token obtained from their IDP service. This use case applies to any IDP (AD FS or other kinds of IDPs).

Tenant-to-Tenant

This case is sometimes referred to as “tenant to tenant” because both the SP and IDP are Delinea tenants. Your business partners access the resources/applications by passing a SAML token obtained from their Delinea IDP tenant to their Delinea SP tenant.



Responsibilities

Partners are responsible for the following:

- Providing you with their IDP metadata.
- Providing you with the group attribute value(s) that they will pass in their SAML tokens. See "Understanding Group Attribute Values to Roles Mapping" below.
- Configuring their IDP to pass SAML tokens to you:
  - If your partner is using another Delinea tenant, they can easily do this by deploying the Delinea B2B SAML application. See Custom SAML applications.
  - SAML payload must contain a raw digital key in the signature element.

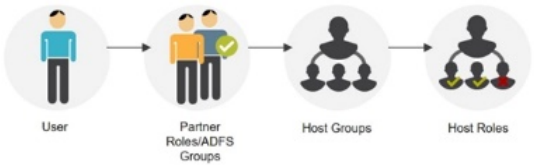
Service Providers (SPs) are responsible for the following:

- Providing the SP metadata to your partner. See "Providing the Service Provider Metadata" on page 271.
- Adding the partner in Admin Portal. See "Add a Partner" on the next page. You will need the IDP metadata and the group attribute value from your partner before you can complete this task.
- Assigning your groups to roles in Admin Portal. See "Assigning Host Groups to Roles" on page 270.
- Mapping of the global group attribute (for all your partners) to your groups. See "Mapping of Global Group Attributes" on page 271.
- Specifying multi-factor authentication (MFA) for partner logins. See "Specifying Partner MFA Requirements" on page 271.

Understanding Group Attribute Values to Roles Mapping

As part of managing their users, partners typically assign them role-based values (also known as group attribute values), such as Sales Managers, Service Managers, etc. However, we do not have visibility into their user directories and one partner may name the value "Sales Managers" while another partner may name it "SalesTeamManagers". To organize these group attribute values, we have created a group construct in the

federated directory service. As the systems administrator in the host tenant, you can create host groups (for example "Mgrs-Sales" group) in which to map the group attribute values (for example the "Sales Managers" and "SalesTeamManagers" values). This host group can then be added to roles in your tenant. The diagram below demonstrates this flow.

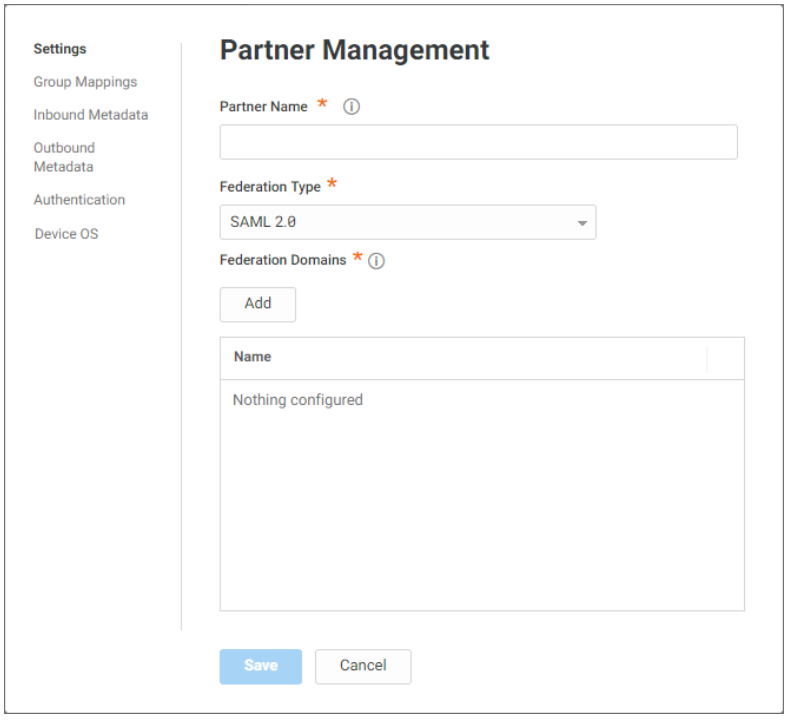


Add a Partner

Add the partner in **Admin Portal** to enable sharing on your end. You will need the group attribute values and IDP metadata from your partner to finish the configuration.

Creating a partner

1. Log in to Admin Portal.
2. Click **Settings**, **Users**, **Partner Management** and **Add**.



3. Enter a unique partner name.
4. Ensure your SAML file includes the required elements.

   SAML 2.0 is automatically selected because we currently only support this federation type.

   The following attributes are consumed by federations with other Cloud customers.

`userprincipalname` is a mandatory attribute that needs to be configured in the IDP SAML configuration.

Additional attributes are supported and can be configured with the partner IDP SAML configuration. These can also be configured on the Service Provider side with the B2B application template.

Mandatory attribute:

`userprincipalname` (mandatory)

Additional supported attributes:

- `DisplayName`
- `Description`
- `Email`
- `Group`
- `HomeNumber`
- `LoginName`
- `MobileNumber`
- `OfficeNumber`

  For example:

```
setAttribute("userprincipalname", LoginUser.Get("userprincipalname"));
```

5. Click **Add** associated with the Domain Name field to enter a unique domain name.

   This domain name will be used as the login suffix for all partner users. It allows Delinea to recognize users coming from a specific IDP and redirects them accordingly. For example, you may want to use the business partner company name (for example companyABC.com) as the domain name.
6. Click **Add** to add the domain name to the table.
7. Click **Group Mappings** > **Add** to create a mapping of the group attribute values to your groups.

   For example, create a group mapping for partner roles for other Delinea tenants, or federated groups.

   The SAML attribute can be multi-valued and must be from the Identity Provider to Delinea.
8. Enter the federated group into the **Group Attribute Value** column. This is your mapping name.
9. Select an existing group in the **Group Name** column or enter a new name.

   Once you save, the service creates the group. This group can then can be assigned to roles.

   Note: You will see the group name when you assign a member to a role, and select only the **Groups** check box.

   This step maps the federated groups (information you should have received from your partner) to your groups. For details, see "Assigning Host Groups to Roles" on page 270.
10. Click **Custom Mappings** > **Add** to create a custom mapping of the user attribute values.

This maps users with the specified attribute name and value to the selected group. Users mapped to groups are given the same admin rights as the group.

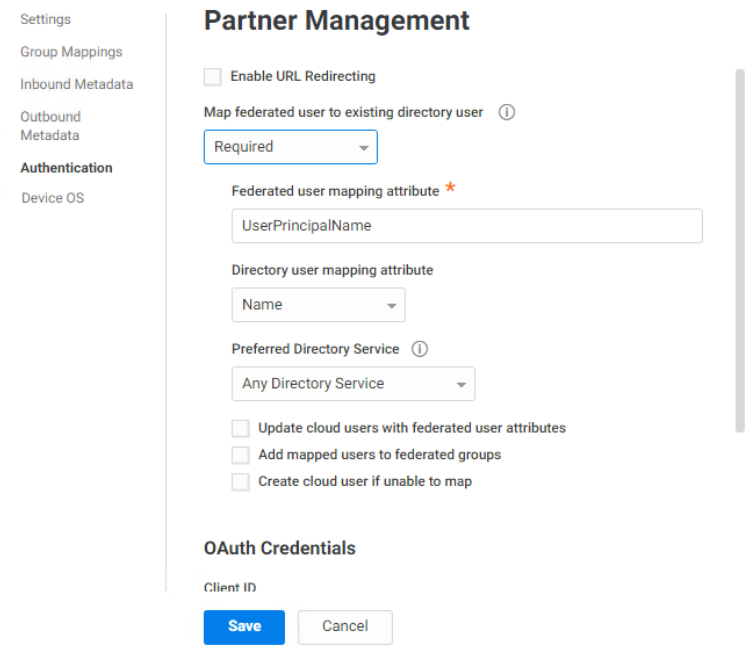
11. Click **Inbound Metadata** to configure IDP settings (using the IDP metadata you received from your partner) for this partner using one of the following options:
    - Option 1: Upload the IDP configuration from URL. To use this option, paste the Identity Provider SAML Metadata URL provided by your partner.
    - Option 2: Upload IDP configuration from a file. If your partner provided the Identity Provider SAML Metadata in an XML file, you can upload it here.
    - Option 3: Manual Configuration. Manually enter the relevant information. This is not a recommended option.
12. Click **Outbound Metadata** to provide IDP configuration settings (using the IDP metadata to send to your federating partner) for your partners using one of the following options:
    - Option 1: Service Provider Metadata URL. Copy this link and paste at the partner IDP SAML configuration.
    - Option 2: Download Service Provider Metadata. Upload this file at the partner IDP SAML configuration.
    - Option 3: Manual Configuration. Copy and paste this information at the partner IDP SAML configuration.
13. Click **Authentication** to configure mapping federated users to existing directory users.

    By default, when a federated user logs in, a new user is created in the Delinea Directory, even if a user already exists in a source directory (Delinea Directory, AD, LDAP, or Google) that has the same uuid or username. This feature maps the authenticated user to an existing user (if possible) before creating a new Delinea Directory user. By default, assertions of the federated user are ignored in favor of the attributes of the mapped user.

    a. (This step is optional) Select **Enable URL** redirecting if you want incoming federated users to be redirected to the target URL (as defined by the RelayState).

       If you enable URL redirecting, you can also limit redirection to a RelayState matching the URL pattern. If the field is empty, all URLs are allowed. The URL pattern is a wildcard pattern starting with https://. For example, https://www.example.com*.

    b. Select **Optional** or **Required** in the **Map federated user** to existing directory user drop-down menu to enable the feature.



- Selecting **Optional** means authentication of a mapped federation user results in the user of the mapped directory service. If a user cannot be mapped, a new Federated user is created.
- Selecting **Required** means the user of a federation will authenticate as the matching user of another directory service. If no match is found, login is denied. If **Create cloud user if unable to map** is also enabled, a matched Delinea Directory user is created and login is permitted.

c. (This step is optional) Enter a federated user mapping attribute.

   The default value is `UserPrincipalName`, since it is a required assertion.

   The federated user mapping attribute must be in the SAML assertion and map to either the **Name** or **Uuid** source directory attributes. If you change this value to an attribute that is not in the assertion and/or does not map to a unique attribute in a source directory, the mapping will fail.

d. Select a directory user mapping attribute; either **Name** or **Uuid**.

e. (This step is optional) Select a preferred directory service to search first for existing users. After the preferred directory service, remaining directory services are searched according to their creation date.

f. (This step is optional) Select **Update cloud users with federated user attributes** to update a mapped Delinea Directory user with the federated assertions.

Adding a Microsoft Azure Partner

For information on adding a Microsoft Azure partner, see "Entra ID Integration with PAS/Cloud Suite" on page 1096.

Adding an Okta Partner

For information on adding an Okta partner, see "Integration with Okta" on page 1106.

Authenticating to Servers for Federated Users

Since many customers use Okta as the main authentication directory, this example will use Okta to explain how to set up Delinea PAS and Delinea Client so that you can authenticate to servers managed by Delinea with your users.

1. From the Admin Portal navigate to **Resources** > **Systems**.
2. Right-click the system you want to use and click **Enter Account**. This will open a new window, enabling authentication into the system.
3. Authenticate into the server using your login credentials. The logged in user is "local" to the server.

   This manages the back channel between Delinea Client, PAS and the server, and therefore requires you to update your **Admin Portal** settings with your server information.
4. Retrieve the relevant information from Okta.
   a. Set up an App in Okta.

      Note: The app must be a "Native App" that uses **OpenID Connect** as the Sign-On Method.

      The Native App will generate the following:

      - Client ID
      - Client secret
      - Token URL - This is the default Authorization Server. For Okta, you can find this in the Okta Developer Console for your tenant under **API / Authorization Servers** > **Metadata URI**. The Token URL is listed under the token_endpoint variable.

        Save this information, as you will need to use them in the **Admin Portal**.

   b. Ensure a default Scope is set up in the **Scopes** tab for your **Authorization Server**.
5. Return to the Admin Portal and navigate to **Settings** > **Users** >**Partner Management**.
6. Click **Add** to add a new partner.
7. On the Settings tab, Set the **Federation Type**, **Signature Type**, and **Federation Domains**.
8. Click the **Authentication** tab and enter the **Client ID** and **Secret** you copied from your server and fill in the **Token URL**.

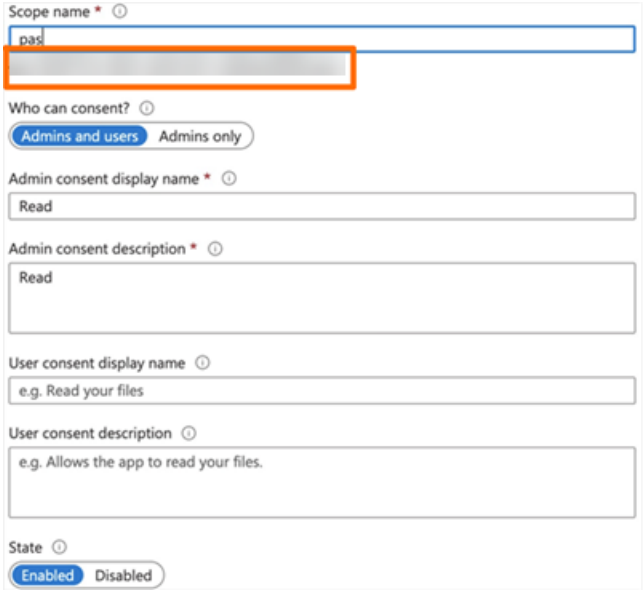
Adding Entra ID as a Federated Partner

If Entra ID is set up as a federated partner, then users can use their Entra ID credentials to log in to enrolled systems. To do this, you first configure Entra ID, then you set up Entra ID as a federated partner in PAS.

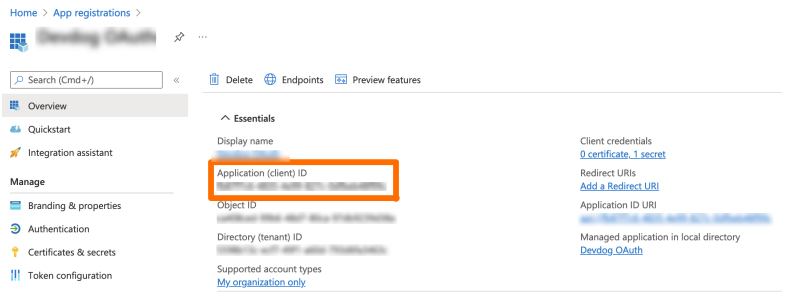
Step 1: Configure the OAuth Resource in Entra ID

1. Navigate to the **Microsoft Azure Portal** and authenticate.
2. Navigate to **Azure Active Directory**.
3. Click **App Registrations**, then click **New Registrations**.
4. Enter 'OAuth Resource' or a similar value as the **Name**.

5. Verify that the **Supported Account Type** is set to **Single Tenant**.
6. Click **Register**, then click **Expose** on API, then click **Add A Scope**.
7. Enter 'pas' as the Scope name.
8. Select **Admins and Users** as who can consent.
9. Enter a display name for the scope. (For example: Read)
10. Enter a description for the scope. (For example: Read) Copy and paste the api://.../pas address generated here for later use:

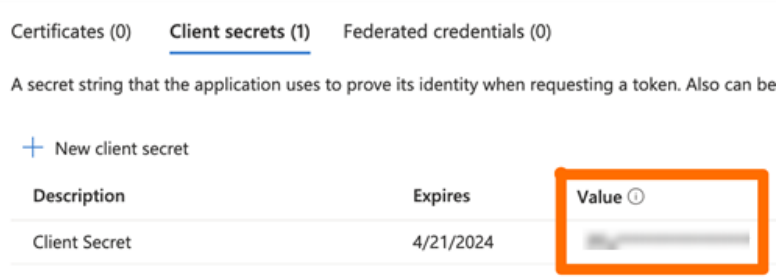


11. Click **Add Scope** .
12. Click **Save**.
13. Go back to the **Overview** screen and copy and paste the **Application (client) ID** for later use:

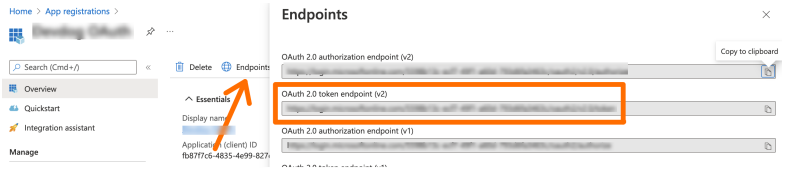


14. Click the link under **Client Credentials** to generate a secret.
15. Under **Client Secrets**, click **New Client Secret**.
16. Enter a description and expiration date.

17. Once created, copy and paste the value of the secret for later use. If you close this window and open it later, you won't be able to copy the secret value:



18. Go back to the **Overview** page, click **Endpoints** and copy the value of the OAuth 2.0 token endpoint (v2) item:



Step 2: Set up Entra ID as the Federated Partner

1. In the **Settings/Users/Partner Management** screen, open **Entra ID Federation** setting.
2. On the **Authentication** screen, paste the values of the following:
   - **Token URL**
   - **Client ID**
   - **Secret**
   - **Scope**

Assigning Host Groups to Roles

For the host groups (those listed in the Group Name column of the Settings, Users, Partner Management, Group Mappings page) to have access to relevant applications and rights, you need to assign them to the relevant roles.

To assign the groups to roles:

1. Log in to Admin Portal.
2. Click **Roles** and select an existing role or create a new one.
3. Click **Members**, **Add** and search for the group.

   In the Source area, you must have the FDS user source selected to see the federated users/groups. Groups from federated services have the icon/FDS label associated.
4. Select the group and click **Add**.
5. Click **Save**.

Mapping of Global Group Attributes

You can create a mapping of global group attributes values (i.e. partner roles for Privileged Access Service tenants, or groups for partners using ADFS) for all your partners to your specified groups. If the system encounters conflicts, the individual group attribute mapping takes priority.

To map global group attributes to your specified groups:

1. Log in to Admin Portal.
2. Click **Settings** > **Users** > **Partner Management** > **Global Mappings**.
3. Enter the global partner role or ADFS group (ADFS federation) into the Group Attribute Value text box, then either select an existing group in the Group Name text box or enter a new name.

   You do this to map global partner roles/ADFS groups (information you should have received from your partners) to your groups. Each group needs to be a member of at least one role in your tenant. See "Assigning Host Groups to Roles" on the previous page.
4. Click **OK**.

Providing the Service Provider Metadata

Provide your partner with your service provider metadata.

To get the service provider metadata:

1. Click **Settings** in Admin Portal.
2. Click **Users > Partner Management**.

   If you have not started creating the partner profile, then click **Add** to access the necessary information. If you have an existing partner, you canlook at that partner's information for the service provider metadata. Thisinformation stays consistent across all partners. In other words, you provide the same metadata information to all your partners.
3. Click **Outbound Metadata** and use one of the three options to get the metadata information.

Specifying Partner MFA Requirements

This configuration is optional for Service Providers (SP).

As a SP, you can require that your business partners meet additional authentication requirements before they can access the resources/applications hosted on your Delinea tenant. For example, you can require that your partner authenticate by answering a security question. This additional requirement ensures that the partner user is using multi-factor authentication (MFA) to access your Delinea tenant.

To specify additional authentication requirements:

1. Login to Admin Portal.
2. Click **Access > Policies**.
3. Select the relevant policy set.
4. Click **Login Policies > Centrify Portal**.

5. Define the authentication requirements you want your partner users to meet. See "How to Define Authentication Requirements" on page 280

   Note: We recommend that you do not define password as one of the additional authentication mechanisms because Privileged Access Service assumes that your partners are logging in using a username/password. If you specify password as one of the authentication mechanism, it will be ignored. For example, if you choose an authentication profile with phone call and password as the authentication mechanisms, the partner user will only be authenticated using phone call.

6. Select the **Apply additional authentication rules to federated users** check box.
7. Click **Save**.

Troubleshoot Account Lockout

Symptoms: Active Directory users are locked out of their Delinea account but the failed login information in **Admin Portal** > **Access** > **Users** > **Activity** does not indicate any failed logins.

Possible solution: Check the external authentication methods to Active Directory, for example IMAP, WS-Trust, or SMTP authentications. Delinea does not record these authentication attempts but because their Active Directory accounts are locked out, they also cannot authenticate into Delinea.

Reference Content – User Accounts

You can use the reference content as supplemental information to the “How To” content.

User Account Sources

Privileged Access Service supports user accounts from multiple identity stores/account sources -- Active Directory or another LDAP-based service, G-Suite (Google), Privileged Access Service. On the User page, the Source column indicates the ID repository for that user account.

- Active Directory/LDAP

  These users are authenticated using their Active Directory/LDAP accounts. The Active Directory/LDAP account domain is shown in the parenthesis.

  Privileged Access Service does not replicate Active Directory/LDAP accounts and their attributes in the Privileged Access Service. Instead, the new useraccounts are brought into Privileged Access Service when the user registers a device or opens a password-protected application.

  If you have multiple connectors managing multiple, independent domain trees or forests, the Source column also shows the source domain.

  To use Active Directory/LDAP as a source, you must install the connector. See How to install a Delinea Connector for the details.

  You must add an Active Directory/LDAP accounts to a role to deploy applications to those users. You can add either the user ActiveDirectory/LDAP accounts or the user Active Directory/LDAP groups to the role. See "Assigning Users to Roles" on page 228 for the details.

- G-Suite

  These users are authenticated using their G-Suite (Google) accounts.

Privileged Access Service does not replicate G-Suite accounts and their attributes in the Privileged Access Service. Instead, the accounts arereferenced when the user registers a device or opens a password-protected application.

To use G-Suite as an account source, you must add it to Privileged Access Service. See "How to Add a Directory Service" on page 256.

- Delinea Directory

  Delinea Directory: Privileged Access Service includes this built-in identity repository. With this option, the Privileged Access Service accountis used to authenticate users. These users have a Delinea Directory account and the account information resides in Privileged Access Service only.

  You must create Delinea Directory accounts explicitly before these users can register a device. You can add Delinea Directory accounts individually or in bulk from a CSV file or Excel spreadsheet.

  Delinea Directory: Privileged Access Service includes this built-in identity repository. With this option, the Privileged Access Service account is used to authenticate users.

You can use all identity stores simultaneously. For example, if you decide to use Active Directory/LDAP as your primary identity store, the Privileged Access Service can provide a convenient supplemental repository for the following types of users:

- Emergency administrators: If there is ever a network break down to the Active Directory domain controller, no one with just an ActiveDirectory/LDAP account can log in. However, if you create administratoraccounts in Privileged Access Service, these users can log in to Admin Portal launch web applications.
- Temporary user: Some organization's security policy can make adding a short-term user to Active Directory/LDAP a complex and time-consuming task.If you have a temporary worker who needs access to just the applications youdeploy through the Privileged Access Service, it may be simpler to add the account to Privileged Access Service.
- Contractors or less-trusted users: Sometimes you do not want users to have the full set of privileges and access rights an Active Directory/LDAPaccount provides. In this case, you create the account in the Privileged Access Service only.

To avoid users logging in to unintended repository accounts and other account related confusion, we recommend that you do not create duplicate accounts (same user name/password) in both the Delinea Directory and Active Directory/LDAP.

User Account Statuses

After a user account has been created and brought into Privileged Access Service, the platform assigns it a status. These statuses are displayed on the User page for each user account.

Status	Indicates
Active	The user has either logged in to one of the portals or registered a device.

Status	Indicates
Invited	An administrator has sent an invitation to register a device, however, the user has not responded. You can send an invitation when you create a Delinea Directory account or separately to accounts in all sources using the Invite User button. The **Last Invite** column indicates the date and time of the most recent invitation. When you add accounts to Privileged Access Service using Bulk import, Admin Portal automatically sends an email invitation to all new accounts by default.
Not Invited	The account was created in Privileged Access Service but no email invitations have been sent. Successfully provisioned users appear on the Users page with a status of Not Invited.
Suspended	The user account is locked. There are several reasons why an account is locked, for example, it could locked by the system administrator or the user has reached the maximum number of log-in attempts. See "How to Configure User Self-Service Options" on page 241 for account unlock options.

User Management Commands

Admin Portal provides several user management commands. They are displayed when you right-click the name on the Users page and in the **Actions** menu on the account's details page.

Command	Result
Delete	Deletes a Delinea Directory account from Privileged Access Service. The user is no longer listed on the Users page and is no longer able to log in to the Admin Portal or Admin Portal. For Active Directory/LDAP user accounts, the deleted account is only removed from the Users page. You must use Active Directory Users and Computers to delete the Active Directory/LDAP account. See "How to Delete User Accounts" on page 233 for more information.
MFA Unlock	Suspends multi-factor authentication for 10 minutes. Multi-factor authentication requires users to perform additional steps (such as verify their identity by email or phone call) to log in to the Admin Portal and Admin Portal. If the user is having trouble logging in, select the user and select this action to let the user log in with just a user name and password.
Send email invite for user profile setup	Sends an email to the selected users with their login account name.
Reload	Updates the user's rights immediately to put into effect any changes you have made to the account–for example, if you added the user to a new role or changed the user's administrative privileges. Use this command immediately after modifying the user's role or rights.
Set Password	Prompts you to reset the user's Privileged Access Service account password. In the window that appears, you enter a new password for the user.

Notifying Users with Active Directory/LDAP Accounts

Users with Active Directory/LDAP accounts log in to the admin portal and register devices using their Active Directory/LDAP credentials.

To get Active Directory/LDAP users started with Privileged Access Service, you can send them an invitation or you can provide the following URL to the users and tell them to use their Active Directory/LDAP credentials to log in:

https://cloud.centrify.com/my

They use the same credentials to register devices.

Simplifying logging in to Privileged Access Service portals for Active Directory/LDAP accounts

Users with Active Directory accounts can log in to the Admin Portal without entering their user name and password from computers that are within your organization's intranet. For example, you can log in to Admin Portal without entering your credentials by appending the login suffix to the portal's URL as follows:

https://cloud.centrify.com/manage?customerid=<loginsuffix>

If you have not yet defined any other login suffixes, you can use the default suffix—your Active Directory account's UPN suffix. For example, if your domain name is abcorp.com, you would enter the following URL to log in without entering your user name and password:

https://cloud.centrify.com/manage?customerid=abcorp.com

See "How to Use Login Suffixes" on page 236 to learn about login suffixes.

Similarly, users can log in to the Admin Portal by adding the login suffix to their URL. In this case the syntax is as follows:

https://cloud.centrify.com/my?customerid=<loginsuffix>

Both of these methods use Integrated Windows Authentication to authenticate the user using their Active Directory credentials and require the user to be on your organizations intranet. You may need to reconfigure the default Integrated Windows Authentication settings and define IP Addresses on your Delinea Connector to use this feature. See "How to Configure Integrated Windows Authentication" on page 309 to configure a Delinea Connector.

You can also define a login suffix as an alias for a long Active Directory/LDAP UPN suffix. See "Creating an Alias for Long Active Directory Domain Names" on page 238 for the details.

Using Search and Sets

You use the user search and Sets (sets of users) to find specific users. User search and sets can be found in **Admin Portal > Access > Users**.

Most of the user sets are self explanatory. The following sets require more explanations:

- All Active Users: Users who have logged in to or been invite to Privileged Access Service.
- All Invited Users: Users who have not logged in to or been invite to the Privileged Access Service.
- All Non-Active Users: Users who have been application provisioned but have never logged in.

User state (active or suspended) does not have any impact on these queries.

Reference Content – Roles

You can use the reference content as supplemental information to the "How To" content.

Predefined Roles

You use roles to assign applications, permissions, and policies to separate sets of users. Your role must have the Roles Management administrative right to view, add, and modify roles. See "Creating Privileged Access Service Administrators" below for the details.

Privileged Access Service provides the following predefined roles:

- **Everybody**: By default, all Privileged Access Service users are assigned to this role. For example, all users that are added to the DelineaDirectory by using bulk import are added to the Everybody. When you add anindividual user, the default setting is to add the account to the Everybody role. To exclude a user from the Everybody role, select the **Is Service User** option on the user Account page.

  It is best practice to assign most users to the Everybody role. However, there are users you may not want to have in the Everybody role; for example, temporary users such as service contractors.

- **Invited Users**: This role is created when you use the **Invite Users** button and select **InvitedUsers** as the Role.

  If you do not use the Invite users button or select the Invited Users role when you invite a user, this role is not created.

- **sysadmin**: This role grants full access to all Admin Portal settings. By default, the Delinea Directory account for the user who signed up for Privileged Access Service is a sysadmin role member. You cannot delete or rename the sysadmin role.

  Only sysadmin role members can add more users to the sysadmin account.

- **Read only Administrator**: This role is automatically created when you enable read-only access for a support technician.

  You can delete the Readonly Administrator role after the time period expires.

Creating Privileged Access Service Administrators

You use roles to create Privileged Access Service administrators. Only users in the sysadmin role and users in roles with administrative rights can open the Admin Portal.

To create a Privileged Access Service administrator, you create a role, assign one or more Admin Portal administrative rights, and then add users to the role. The administrative rights let you define roles with separate application, user, device, report, and role management permissions.

For example, you can create a role that limits the administrator to managing applications and application-to-roles assignments only. In this role, the administrators can perform all the functions on the Apps page and read-only access to the Users and Roles pages. Similarly, you can create administrative roles with just device, user, and report management permissions.

System Administrator Role Permissions

The sysadmin role members have access to all Admin Portal tabs and the Delinea Connector Configuration Program settings. They are also the only administrators who can perform the following tasks:

- Add users to or remove them from the sysadmin role.
- Modify the Account Customization tab on the Settings page in Admin Portal

- Modify connector settings in the Delinea Connector tab on the Settings page in Admin Portal.
- Modify policy sets.
- Create a Discovery Systems profile.
- Grant Global Account permissions.
- Grant Global System permissions.

These rights cannot be assigned to other roles. However, you can add users to the sysadmin role. See "Adding Roles" on page 220.

Note: Discovery jobs run with very high privilege as they update accounts and systems regardless of the access rights associated with the objects. As such, the sysadmin may not want all PAS administrators granted permission for discovery. As such, the sysadmin can create a system discovery profile, and if they choose, explicitly grant rights to view, edit, and run the profile (for example, they can assign all rights to a "PAS Admins" role). Other administrative functions such as Global Account Permissions and Global System Permissions are, similarly, only available to the sysadmin as not all PAS Admins may have rights to assign permissions.

Admin Portal Administrative Rights

The following table describes the administrative rights you can assign to a role. Users cannot log in to the Admin Portal unless they have at least one of the following administrative rights.

If an administrator attempts to perform a task in the Admin Portal for which they do not have the associated administrative right, the Admin Portal displays an error message. In addition, the Admin Portal does not display data if it's not pertinent to the administrator's rights. For example, if the administrator has the Application Management right only, that user is not allowed to change policy settings.

Note: Some administrative rights also grant reporting rights, but only for data that the user has been granted rights to read. Additionally, see the administrative right descriptions below.

Administrative right	Description
Add Cloud Providers	If you also have the "Privileged Access Service User" or "Privileged Access Service Power User" right, this permission grants you the ability to add cloud providers (and their respective accounts) to the service. You have the permission to manage any cloud providers that you add.
Add Databases	If you also have the "Privileged Access Service User" or "Privileged Access Service Power User" right, this permission grants you the ability to add databases (and their respective accounts) to the service. You have the permission to manage any databases that you add.
Add Domains	If you also have the "Privileged Access Service User" or "Privileged Access Service Power User" right, this permission grants you the ability to add domains (and their respective accounts) to the service. You have the permission to manage any domains that you add.

Administrative right	Description
Add SSH Keys	If you also have the "Privileged Access Service User" or "Privileged Access Service Power User" right, this permission grants you the ability to add SSH keys to the service. You have the permission to manage any SSH keys that you add.
Add Systems	If you also have the "Privileged Access Service User" or "Privileged Access Service Power User" right, this permission grants you the ability to add systems (and their respective accounts) to the service. You have the permission to manage any systems that you add.
Admin Portal Login	Access to the Admin Portal.
Application Management	Access to any activities that originate on the Apps page, such as the ability to add, modify, or remove applications. From the Application Settings dialog box, this right also grants the ability to change which roles are assigned to a specific application.
Computer Login and Privilege Elevation	Logging on to Windows, Linux, or UNIX computers where a Cloud Client is installed. This administrative right is only applicable for the computers that are members of an Delinea PAS role with this right.
Device Management	Permission to unregister or delete mobile devices
Federation Management	Permission to create, manage, and delete federation partnerships. See "How to Set Up Business Partner Federation" on page 261 for information on setting up partner federations.
MFA Unlock	Suspend multi-factor authentication for 10 minutes.
MFA Redirect Management	Permission to set MFA redirection for users.
Privilege Elevation Management	Permission to grant privilege elevation access.
Privileged Access Service Administrator	If you add this administrative right to a role, members of the role can add new objects–systems, domains, databases, services, or accounts–to the Delinea PAS. Members of a role with this right become the default owner of the objects that they add. If there's more than one member of the role, each administrator is only the owner of the objects they add by default. Members of a role with this right can perform all administrative tasks on the objects they own.

Administrative right	Description
Privileged Access Service Power User	If you add this administrative right to a role, members of the role can see all objects you add to the Delinea PAS in the Admin Portal. By default, however, members of a role with this right are not granted the Login, Checkout, or Rotate permissions. The system, domain, database, service, or account owner (or a member of the System Administrator role) must explicitly grant the appropriate permissions. Members of this role cannot add new objects to the Delinea PAS.
Privileged Access Service User	If you add this administrative right to a role, members of the role can see the objects on which they have been granted View permissions in the Admin Portal. This administrative right is primarily for users who need some administrative access to a selected set of objects. Members of a role with this right are granted the Login, Checkout, and Rotate password permissions. Members of a role with this right can only perform these tasks for the accounts or systems where they have the View permission. Members of this role cannot add new objects to the Delinea PAS.
Query as a different user	Use this permission to run a query as a different user.
RADIUS Management	Permission to create, manage, and delete the RADIUS server. See "How to Configure Privileged Access Service for RADIUS" on page 323 for information on using the Delinea Connector as a RADIUS server.
Read Only Resource Management	Provides read-only access to Resources (including secrets), Desktop Apps, Global Account Permissions, and Global System Permissions.
Read Only System Administrator	Provides read-only access to some of the Admin Portal tabs. For instance, certain Admin Portal tabs are not available, such as Resources, Desktop Apps, Global Account Permissions, and Global System Permissions. If the user attempts to make a change, an error message is displayed when the user attempts to save the change. If you need to have read-only access to Resources (objects), see **Read Only Resource Management** and **Privileged Access Service Power User** above. **Note**: If you enable read-only access for a support technician, the Delinea PAS creates a temporary account that it adds as a member to this role.
Register and Administer connectors	Register a Delinea Connector in your Delinea PAS account. During the connector installation, the wizard prompts you to enter the account of a user that has the Register connector right. This must be a Delinea Directory account. Make sure the account you specify is a member of a role with this permission.
Report Management	Create, delete, and run reports.

Administrative right	Description
Role Management	Access to any activities that originate on the Roles page, such as the ability to add, modify, or delete roles; this includes the ability to assign rights.
System Enrollment	Permission for non-admin users to register Linux and Windows machines.
User Management	Permission to use the Add User and Bulk User Import buttons to add users and modify Delinea Directory user properties. Additionally, this permission allows users to import and delete OATH tokens.

See "Adding Roles" on page 220 for instructions on how to add administrative rights to a role.

Authenticate

You can use Privileged Access Service to authenticate users for single sign-on to various environments and device types. At the core level, you can specify the authentication mechanisms your users must provide to access Privileged Access Service and deployed applications, as well as if and when multifactor authentication is required. At the more advanced level, Privileged Access Service supports authentication with RADIUS and smart cards.

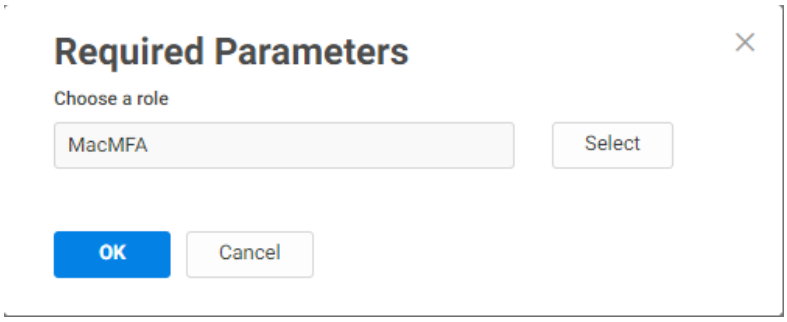
How to Define Authentication Requirements

You can specify what authentication mechanisms your users must provide to access the service, as well as if and when multi-factor authentication is required. For example, you can create a rule to require that users provide a password and text message confirmation code if they are coming from an IP address that is outside of your corporate IP range. To specify this requirement, you need to create a rule and associate it with an authentication profile.

A built-in report is available to view whether users have setup the necessary information for multi-factor authentication challenges. For example, if you plan to use SMS confirmation codes as an authentication factor, you need to make sure all users impacted by the authentication policy have a mobile number associated with their account, otherwise they might be locked out.

1. From the **Reports** page in the Admin Portal, navigate to **Builtin Reports > Security**, and open **User MFA challenge setup status**.

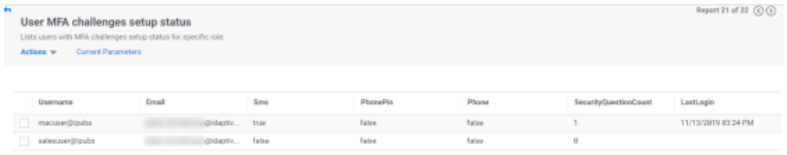
   The Required Parameters window appears.



2. Select the role that will be impacted by your Authentication Policy.

   For performance reasons, run this report on roles with approximately 1,000 users or less.

   The report opens, showing whether your users have configured the required information for authentication factors that could result in lockout if the required information is absent. For example, a user with no associated mobile phone will have false in the SMS column.

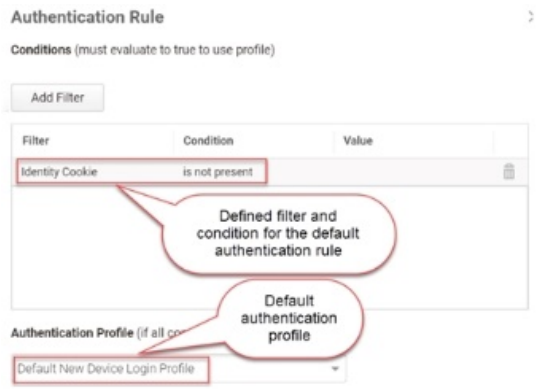


3. Review the report and follow up with users missing required information.

Creating Authentication Rules

Authentication rules define the conditions in which a certain authentication profile is applied. For example, you can create a rule to require that users provide a password and text message confirmation code if they are coming from an IP address that is outside of your corporate IP range. To specify this requirement, you need to create a rule and associate it with an authentication profile.

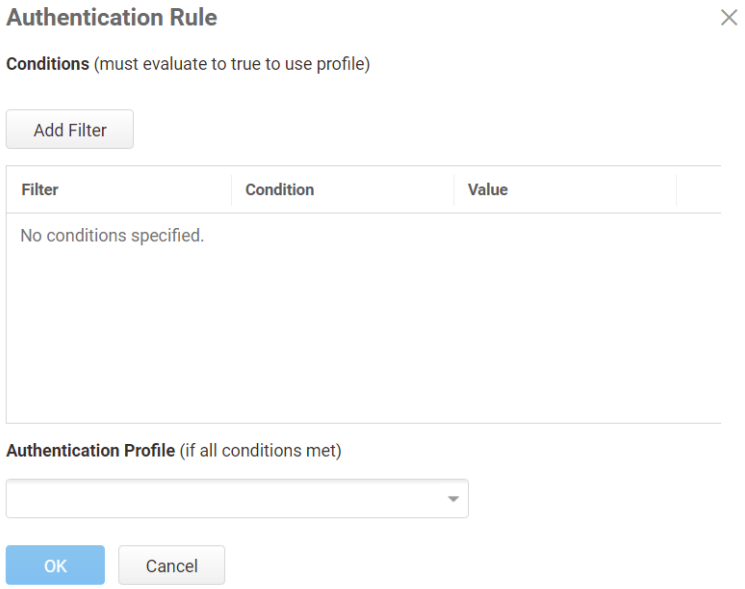
If you do not define any authentication rules, then a default rule and profile is used. This default rule uses the identity cookie not present condition and the Default New Device Login Profile. This profile uses Password for the first challenge and Mobile Authenticator, Text message (SMS) confirmation code, Email confirmation code, or OATH OTP Client for the second challenge with a 12 hours pass-through duration. The following image shows the default authentication rule.



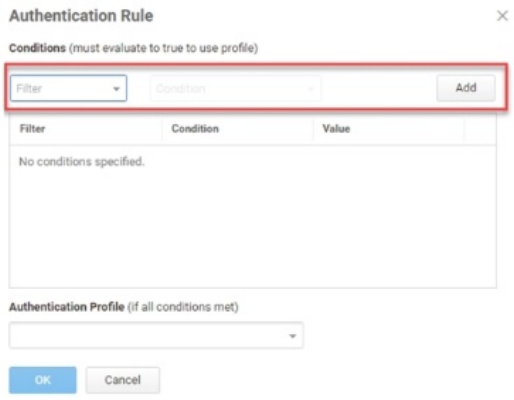
To define an authentication rule:

1. In the Admin Portal, click **Access > Policies**.
2. Click **Add Policy Set** to create a new one.
3. Click **Authentication > Centrify Services**.
4. Select **Yes** in the **Enable authentication policy controls** drop-down.
5. (Optional) Click **Add Rule** to specify conditional access.

   The Authentication Rule window displays.



6. Click **Add Filter** on the Authentication Rule window.
7. Define the filter and condition using the drop-down menus.



   For example, you can create a rule that requires a specific authentication method when users access Privileged Access Service from an IP address that is outside of your corporate IP range. Available filters vary depending on the object they are applied to and features enabled on your tenant. Supported filters are:

Filter	Description
IP Address	The authentication factor is the computer's IP address when the user logs in. This option requires that you have configured the IP address range in Settings, Network, Corporate IP Range.
Identity Cookie	The authentication factor is the cookie that is embedded in the current browser by Privileged Access Service after the user has successfully logged in.
Day of Week	The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.
Date	The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.
Date Range	The authentication factor is a specific date range.
Time Range	The authentication factor is a specific time range in hours and minutes.
Device OS	The authentication factor is the device operating system.
Browser	The authentication factor is the browser used for opening the Privileged Access Service portal.
Country	The authentication factor is the country based on the IP address of the user computer.
Certificate Authentication	The certificate is used for authentication.
For the Day/Date/Time related conditions, you can choose between the user's local time and Universal Time Coordinated (UTC) time.	

1. Click the **Add** button associated with the filter and condition.
2. Select the profile you want applied if all filters/conditions are met in the **Authentication Profile** drop-down.

   The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the**Add New Profile** option. See "Creating Authentication Profiles" on the next page.
3. Click **OK**.
4. (Optional) In the **Default Profile (used if no conditions matched)**drop-down, you can select a default profile to be applied if a user does not match any of the configured conditions.

   Note: If you have no authentication rules configured and you select **Not Allowed** in the **Default Profile** drop-down, users will not be able to log in to the service.

5. (Optional) If you have more than one authentication rule, you can drag and drop the rules to a new position in the list to control the order they are applied.
6. Click **Save**.

If you have more than one authentication rule, you can prioritize them by dragging them. The rule on top has the highest priority.

Creating Authentication Profiles

The authentication profile is where you define the required authentication mechanisms such as password, email confirmation code, mobile authenticator, and so on. You use the authentication profile when you create your authentication rule.

Three default authentication profiles are available out-of-the-box:

- Default New Device Login Profile: Uses Password for the first challenge and Mobile Authenticator, Text message (SMS) confirmation code, Emailconfirmation code, or OATH OTP Client for the second challenge with a 12 hours pass-through duration.
- Default Other Login Profile: Uses Password for the first challenge and no secondary challenge with a 12 hours pass-through duration.
- Default Password Reset Profile: Gives the option for users to use Mobile Authenticator, Text message (SMS) confirmation code, Email confirmationcode, or OATH OTP Client for the first challenge with a 12 hours pass-through duration.

Push notifications to 3rd party services such as email, SMS, and phone calls are subject to a delay that is independent of the Privileged Access Service. If the mobile carrier or mail provider causes a delay in receiving notifications that impact login, we recommend you use a none push authentication mechanism such as OATH token, or Delinea Mobile Authenticator's "Enter code" option which does not rely on a 3rd party service to deliver the message to the device.

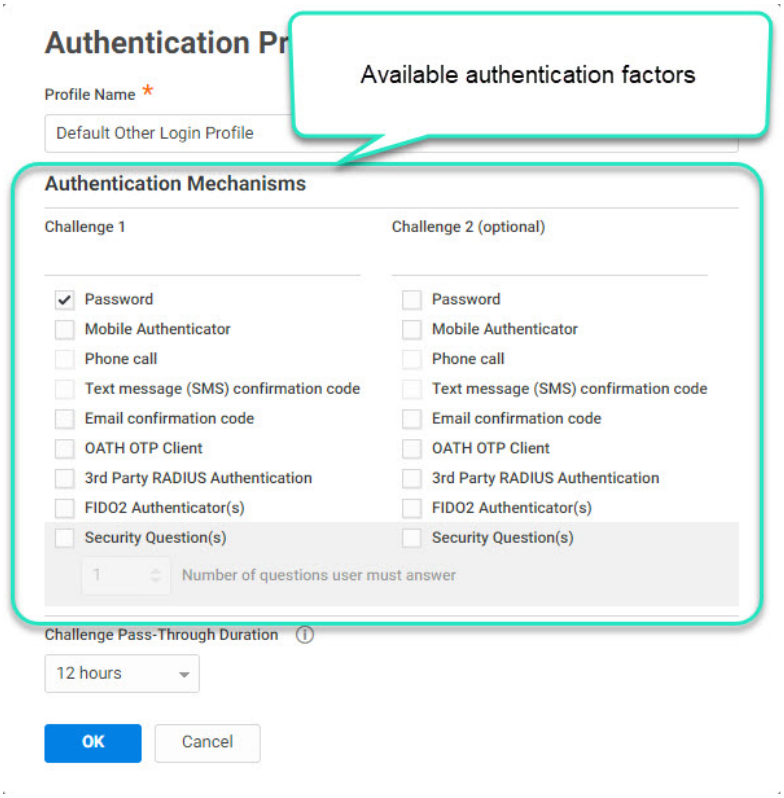
To create an authentication profile:

1. Click **Settings > Authentication**.
2. Click **Add Profile** on the Authentication Profiles page.
3. Enter a unique name for each profile.
4. Select the authentication mechanism(s) you require and want to make available to users.

   Some authentication mechanisms require additional configurations before users can authenticate using those mechanisms. For example, you can requirethat the first challenge be the user's account password. Then for the secondchallenge, users can choose between an email confirmation code, securityquestion, or text message confirmation code. See "Authentication Mechanisms" on page 356 for information about each authentication mechanism.

   If you have multiple challenges, Privileged Access Service waits until users enter all challenges before giving the authentication response (pass orfail). For example, if users enter the wrong password for the firstchallenge, we will not send the authentication failure message until after users respond to the second challenge.

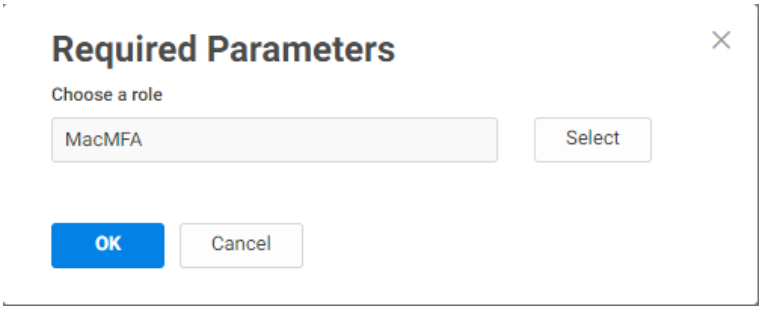
If users fail their first challenge and the second challenge is SMS, email, or phone call, the default configuration is that Privileged Access Service will not send the SMS/email or trigger the phone call. Contact support to change this configuration.



A built-in report is available to view whether users have setup the necessary information for multi-factor authentication challenges. For example, if you plan to use SMS confirmation codes as an authentication factor, you need to make sure all users impacted by the authentication policy have a mobile number associated with their account, otherwise they might be locked out.

a. From the **Reports** page in the Admin Portal, navigate to **Built in Reports > Security**, and open **User MFA challenge setup status**.

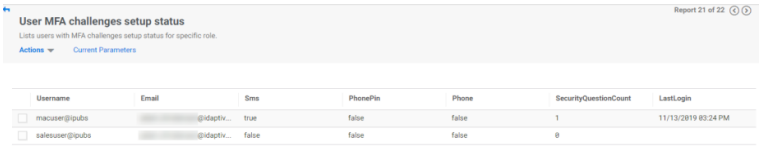
   The Required Parameters window appears.



b. Select the role that will be impacted by your Authentication Policy.

   For performance reasons, run this report on roles with approximately 1,000 users or less.

   The report opens, showing whether your users have configured the required information for authentication factors that could result in lockout if the required information is absent. For example, a user with no associated mobile phone will have false in the SMS column.



c. Review the report and follow up with users missing required information.

5. (Optional) Select the pass-through duration.

   If users have already authenticated using one of the specified mechanism within this duration, then they will not be authenticated again. The default is 30 minutes.

   Important: This pass-through option does not apply to Windows, Linux, Unix, or Mac MFA logins.

6. Click **OK**.

   If you have not created an authentication rule, see "Creating Authentication Rules" on page 281 to create one and associate this profile to it.

Using Authentication Profiles to Secure Access to User Account Settings

In addition to authentication rules, authentication profiles can be used to further secure user access to specified account settings. For example, you can require that before users can modify their personal profile, they must first authenticate using a confirmation code sent via email. The relevant user account settings are:

- Change user password -- "Configuring User Password Change Options".
- Configure an OATH OTP client -- See "How to Configure OATH OTP" on page 347.
- Create a security question -- Using **Admin Portal > Access > Policies > User Security Policies > User Account Settings > Authentication Profile required to set Security Question** drop-down list, you can select an authentication profile with the necessary authentication mechanism defined. This option will require users to authenticate before creating the security question at **Profile** > **Security** page.
- Modify personal profile information -- Using **Admin Portal > Access > Policies > User Security Policies > User Account Settings > Authentication Profile required to modify Personal Profile** drop-down list, you can select an authentication profile with the necessary authentication mechanism defined. This option will require users to authenticate before updating anything on the **Profile** > **Personal Profile** page.

Configuring Authentication for All Conditions

You can require users to always authenticate, regardless of connection factors or conditions. For example, if you create an authentication profile with only the password mechanism selected and assign it to the Default Profile option,

then all users (regardless of the log in computer's IP address and browser identity cookie) will be asked to enter passwords.

To configure authentication for all conditions:

1. Log in to Admin Portal.
2. Click Access > Policies and select the policy you want to edit or click Add Policy Set to create a new one.
3. Click Authentication Policies > Centrify Services.
4. Select Yes in the Enable authentication policy controls drop-down.
5. Select the authentication profile you want applied in the Default Profile drop down.

- The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select **Add New Profile** at the bottom of the drop-down list. See "Preparing Authentication Profiles" on page 352.
- If you have authentication rules configured, then those rules are processed first and users that do not fall under those rules will be processed using the authentication profile selected in the Default Profile.
- **Note:** If you have no authentication rules configured and you select Not Allowed in the Default Profile dropdown, users will not be able to log in to the service.

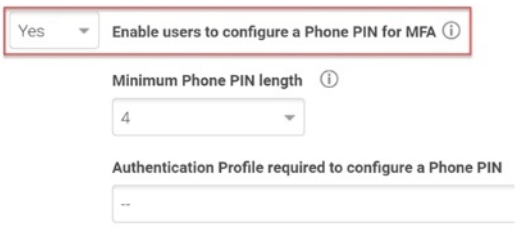
6. Click Save.

Enabling Phone PIN

If you select Phone Call as an authentication mechanism for users, then those users must create a PIN to authenticate into Privileged Access Service using their phones. By default, all users can create a PIN. To enable or disable, see the instructions below. The phone PIN configuration option is only available for new tenants as of 17.10.

To enable or disable a phone PIN:

1. Log in to Admin Portal.
2. Click **Access > Policies** and select the policy you want to edit or click **Add Policy Set** to create a new one.
3. Click **User Security Policies > User Account Settings**.
4. Select **Yes** or **No** in the "Enable users to configure a Phone PIN for MFA" drop-down list.



5. (Optional) Specify the minimum PIN length users must create.
6. (Optional) Specify the authentication profile users must use to configure and edit their PINs.

   The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select **Add New Profile** at the bottom of the drop-down list. See "Creating Authentication Profiles" on page 284
7. Click **Save**.

   Note: Users create their PINs at **Profile > Account > Organization > Phone PIN**.

Enabling Multiple Security Questions

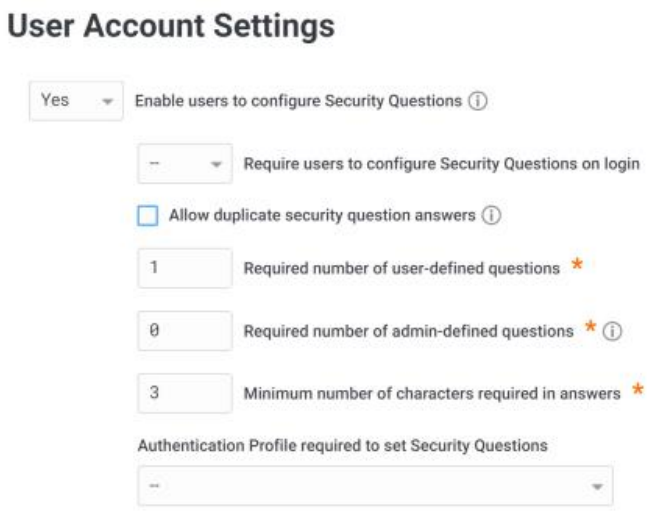
If you select Security Question(s) as an authentication mechanism for users, you must enable the feature for users and the end-users must provide answers to the questions.

To enable the feature:

1. Log in to Admin Portal.
2. Click **Access > Policies** and select the policy you want to edit or click **Add Policy Set** to create a new one.
3. Click **User Security Policies > User Account Settings**.
4. Select **Yes** in the **Enable users to configure security questions** drop-down list.

   Leaving the default selection (--) is equivalent to requiring users to specify one user-defined question and answer.

   Selecting **No** means users will not see the option to answer admin-defined questions or specify/answer user-defined questions.



5. Enter values for the related options.

If the total number of user-defined and admin-defined questions you specify here is greater than the number of questions users must answer, then Privileged Access Service randomly selects questions from the pool of questions containing answers. We will not select questions for which users have not provided answers.

- Require users to configure Security Questions on login: Users can configure security questions.
- Allow duplicate security question answers: Users can enter duplicate answers to different questions if you enable this policy.
- Required number of user-defined questions: Users can enter the questions and answers.
- Minimum number of characters required in answers.
- Authentication profile required to set security questions: (Optional) Specify additional authentication challenges (by selecting an authentication profile) users must provide before they can enter/answer user-defined security questions or select/answer admin-defined questions.

6. Click **Save**.

Writing admin-defined security questions

You can write the admin-defined questions from which users can select, provide answers for, and use for authenticating to Privileged Access Service.

To write the admin-defined security questions:

1. Log in to Admin Portal.
2. Click **Settings > Authentication > Security Questions > Add** button.
3. Enter the question you want made available to users.

   You can only enter one question at time.
4. Click **OK**.

Customizing Session Length and Signed-in Options

A session is that period of time during which Privileged Access Service accepts a previous log in from the same browser for authentication. For example, if the session length is 1 hour and the user logs in and then logs out, that user has 1 hour to access the Admin Portal (from the same browser and machine) without needing to enter his credentials. The default session length is 12 hours.

You can also give users the option to stay logged in, the default setting for this option, and define the maximum hours the user can stay signed in. By default, users do not have the option to stay signed in.

To change the default session length:

1. Log in to Admin Portal.
2. Click **Access > Policies** and select the policy you want to edit or click **Add Policy Set** to create a new one.
3. Click **Login Policies > Centrify Portal**.
4. Select **Yes** in the **Enable authentication policy controls** drop-down.
5. Scroll to **Session Parameters** and enter the number of hours for the session length in the **Hours until identity cookie expires** text box.
6. Click **Save**.

To display “Keep me signed in” on the login screen:

1. Log in to Admin Portal.
2. Click **Access > Policies** and select the policy you want to edit or click **Add Policy Set** to create a new one.
3. Click **Login Policies > Centrify Portal**.
4. Select **Yes** in the **Enable authentication policy controls** drop-down.
5. Scroll to **Session Parameters** and configure the relevant **Keep me Signed In** options.
   a. Select the **Allow “Keep me signed in” checkbox option at log in**option if you want users to see the “Keep me signed in” option when they log in to the Delinea Connector.
   b. Select the **Default “Keep me signed in” checkbox option to enabled**option if you want the “Keep me signed in” checkbox enabled by default for users.
   c. In the associated text box, enter the maximum number of hours users can stay signed in.
6. Click **Save**.

Customizing Session Length and Signed-in Options

A session is that period of time during which Privileged Access Service accepts a previous log in from the same browser for authentication. For example, if the session length is 1 hour and the user logs in and then logs out, that user has 1 hour to access the Admin Portal (from the same browser and machine) without needing to enter his credentials. The default session length is 12 hours.

You can also give users the option to stay logged in, the default setting for this option, and define the maximum hours the user can stay signed in. By default, users do not have the option to stay signed in.

To change the default session length:

1. Log in to Admin Portal.
2. Click **Access > Policies** and select the policy you want to edit or click **Add Policy Set** to create a new one.
3. Click **Login Policies > Centrify Portal**.
4. Select **Yes** in the **Enable authentication policy controls** drop-down.
5. Scroll to **Session Parameters** and enter the number of hours for the session length in the **Hours until identity cookie expires** text box.
6. Click **Save**.

To display “Keep me signed in” on the login screen:

1. Log in to Admin Portal.
2. Click **Access > Policies** and select the policy you want to edit or click **Add Policy Set** to create a new one.
3. Click **Login Policies > Centrify Portal**.
4. Select **Yes** in the **Enable authentication policy controls** drop-down.
5. Scroll to **Session Parameters** and configure the relevant **Keep me Signed In** options.

a. Select the **Allow "Keep me signed in" checkbox option at log in**option if you want users to see the "Keep me signed in" option when they log in to the Delinea Connector.

b. Select the **Default "Keep me signed in" checkbox option to enabled**option if you want the "Keep me signed in" checkbox enabled by default for users.

c. In the associated text box, enter the maximum number of hours users can stay signed in.

6. Click **Save**.

Exempting Users Without Valid Authentication Methods

The Privileged Access Service looks into the user's Active Directory/LDAP or Delinea Directory account for the mobile phone number or email address used for multifactor authentication. Normally, users without a mobile phone number or email address cannot log into Delinea Connector when you enable authentication policy controls.

To exempt users from multifactor authentication when their account does not have a mobile phone number and email address:

1. Log in to the Admin Portal.
2. Click **Access > Policies**.
3. Select the relevant policy or create a new one.
4. Click **Login Polices > Centrify Services**.
5. Enable the **Allow users without a valid authentication factor to log in** setting in the Other Settings section.
6. Click **Save**.

Limiting Multifactor Authentication from the Same Device

You can limit the authentication mechanisms available to users when they use the same mobile device for authentication and accessing the admin portal. Only the following authentication methods will be available from the same mobile device: email, security question, and password. For example, if a user is accessing the admin portal from her mobile phone, then she cannot use that same phone to authenticate via text message, phone call, mobile authentication, or scanning a Delinea Connector generated QR code.

This policy is intended for government agencies needing to fulfill NIST compliance and is disabled by default.

To limit multifactor authentication from the same device:

1. Log in to the Admin Portal.
2. Click **Access > Policies**.
3. Select the relevant policy or create a new one.
4. Click **User Security Polices > Login Authentication**.
5. Uncheck the **Allow additional authentication from same device** setting in the Other Settings section.
6. Click **Save**.

Limiting Multifactor Authentication from the Same Device

You can limit the authentication mechanisms available to users when they use the same mobile device for authentication and accessing the admin portal. Only the following authentication methods will be available from the

same mobile device: email, security question, and password. For example, if a user is accessing the admin portal from her mobile phone, then she cannot use that same phone to authenticate via text message, phone call, mobile authentication, or scanning a Delinea Connector generated QR code.

This policy is intended for government agencies needing to fulfill NIST compliance and is disabled by default.

To limit multifactor authentication from the same device:

1. Log in to the Admin Portal.
2. Click **Access > Policies**.
3. Select the relevant policy or create a new one,
4. Click **User Security Polices > Login Authentication**.
5. Uncheck the **Allow additional authentication from same device** setting in the Other Settings section.
6. Click **Save**.

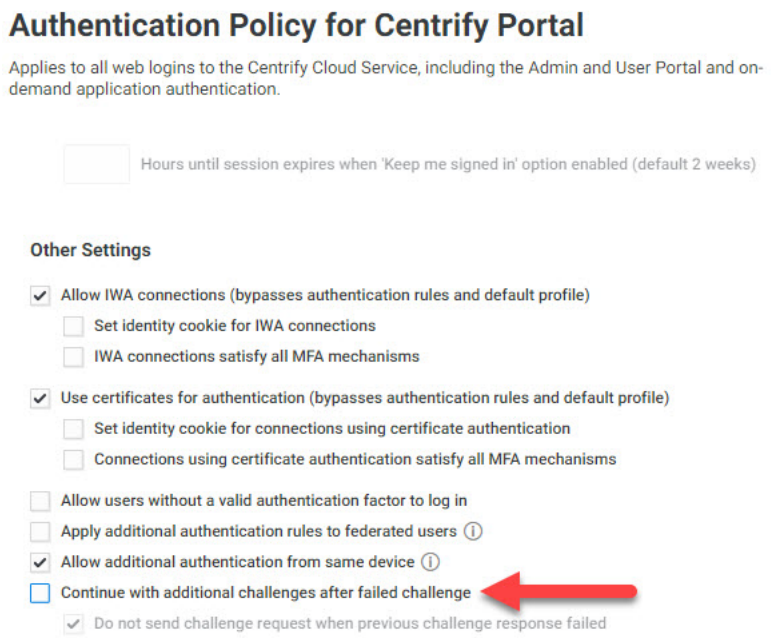
Notifying Users After the First Failed MFA Challenge

The default Privileged Access Service MFA behavior is to allow users to step through all the relevant MFA challenges before we notify them of their failed authentication attempt. For example, if your authentication policy is configured to use password and Email confirmation code, then even if users enter the wrong password during log-in, we still send the email confirmation code. After the last relevant MFA challenge, we notify users of their failed authentication without identifying the failed challenge. However, you can configure Privilegedage Access Service to notify users of their failed authentication after the first failed challenge.

To notify users of a failed authentication after the first failed challenge:

1. Log in to Admin Portal.
2. Click **Access > Policies** and select the policy you want to edit or click **Add Policy Set** to create a new one.
3. Click **Login Policies > Centrify Portal**.
4. De-select the “Continue with additional challenges after failed challenge” policy checkbox.

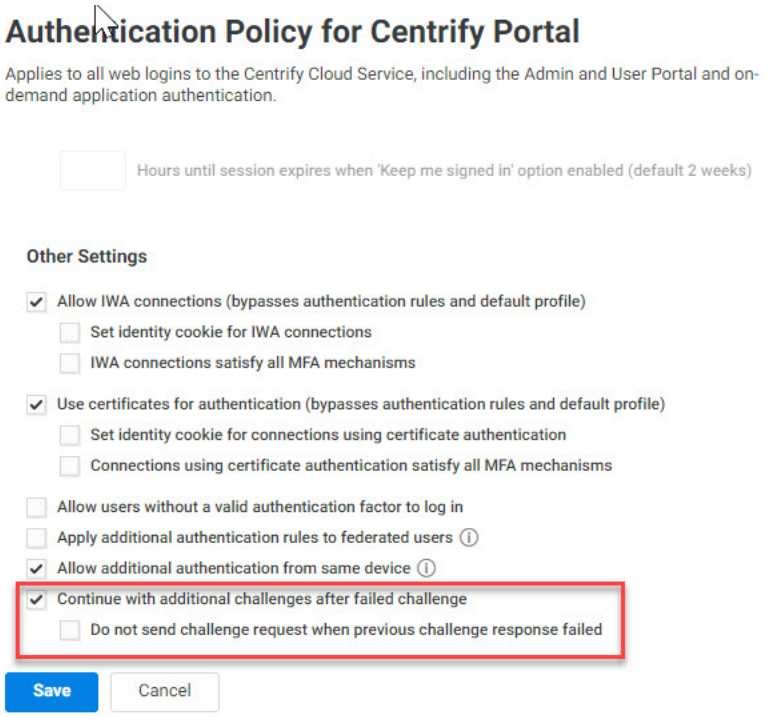
   Users will receive a failed authentication attempt message after the first failed challenge. Privileged Access Service will not send additional authentication challenges.



5. Click **Save**.

Optional Configuration for the Default MFA Behavior

You can configure Privileged Access Service to handle the default MFA behavior (allow users to step through all the relevant MFA challenges before we notify them of their failed authentication attempt) differently based on the challenge type. If you deselect the “Do not send challenge request when previous challenge response failed” check box but leave the “Continue with additional challenges after failed challenge” check box selected, there are two possible scenarios after users have failed an authentication challenge.



Scenario 1: The next authentication challenge requires Privileged Access Service to send information back to the users, such as email, SMS, or phone call. In this scenarios, users will not receive the necessary information and the authentication session fails. Users must wait until the authentication session times out and try again.

Scenario 2: The next authentication challenge does not require Privileged Access Service to send information back to users, such as a security question. In this scenario, users can proceed with the challenge (for example, answer the security question). After all relevant challenges have been satisfied, we notify users of their failed authentication without identifying the failed challenge.

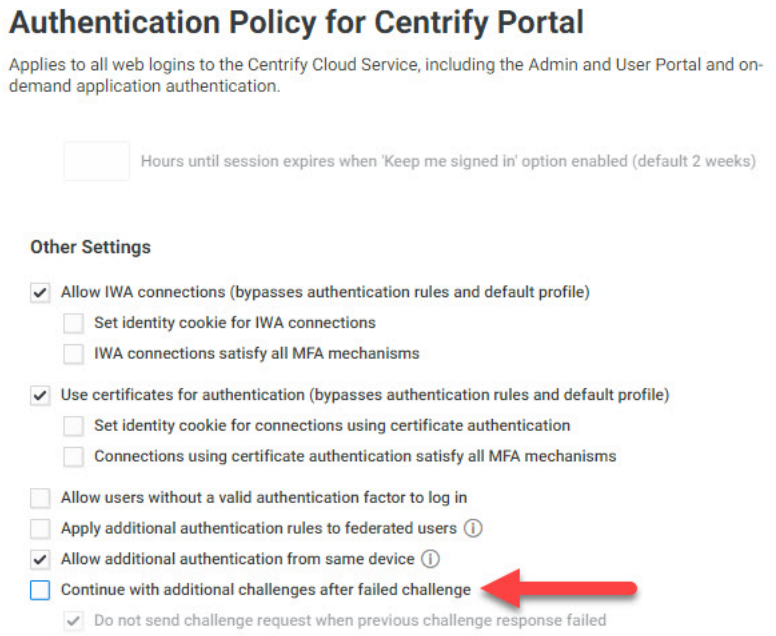
Notifying Users After the First Failed MFA Challenge

The default Privileged Access Service MFA behavior is to allow users to step through all the relevant MFA challenges before we notify them of their failed authentication attempt. For example, if your authentication policy is configured to use password and Email confirmation code, then even if users enter the wrong password during log-in, we still send the email confirmation code. After the last relevant MFA challenge, we notify users of their failed authentication without identifying the failed challenge. However, you can configure Privileged Access Service to notify users of their failed authentication after the first failed challenge.

To notify users of a failed authentication after the first failed challenge:

1. Log in to Admin Portal.
2. Click **Access > Policies** and select the policy you want to edit or click **Add Policy Set** to create a new one.
3. Click **Login Policies > Centrify Portal**.
4. De-select the “Continue with additional challenges after failed challenge” policy checkbox.

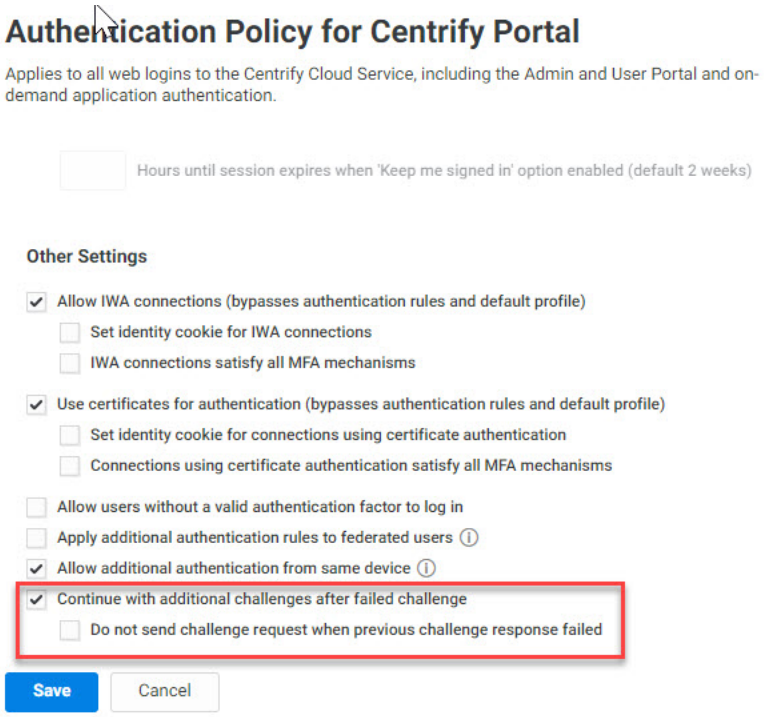
Users will receive a failed authentication attempt message after the first failed challenge. Privileged Access Service will not send additional authentication challenges.



5. Click **Save**.

Optional Configuration for the Default MFA Behavior

You can configure Privileged Access Service to handle the default MFA behavior (allow users to step through all the relevant MFA challenges before we notify them of their failed authentication attempt) differently based on the challenge type. If you deselect the “Do not send challenge request when previous challenge response failed” check box but leave the “Continue with additional challenges after failed challenge” check box selected, there are two possible scenarios after users have failed an authentication challenge.



Scenario 1: The next authentication challenge requires Privileged Access Service to send information back to the users, such as email, SMS, or phone call. In this scenarios, users will not receive the necessary information and the authentication session fails. Users must wait until the authentication session times out and try again.

Scenario 2: The next authentication challenge does not require Privileged Access Service to send information back to users, such as a security question. In this scenario, users can proceed with the challenge (for example, answer the security question). After all relevant challenges have been satisfied, we notify users of their failed authentication without identifying the failed challenge.

How to Set Authentication Security Options

You can configure additional authentication security setting in the Admin Portal. The following configuration options are available from **Settings > Authentication > Security Settings**:

- Use the **Securely capture users' passwords at login** check box to capture user passwords using strong encryption.

  After this option is enabled, Privileged Access Service captures user passwords (using symmetric encryption with AES algorithm) the next time theylog in. By default, Privileged Access Service does not capture userpasswords. However, you might want to capture user passwords to supportaccount mapping options for user password applications or to provision userpasswords for supported applications. Unless capturing user passwords isrequired for a specific feature, Delinea recommends leaving this feature disabled.
- Use the **Enable forgot username self-service at login** check box to allow users to retrieve their forgotten username. Users will be prompted to enteran email address to which the username will be sent if a Privileged AccessService account is found that matches the email address. Refer to "How to Customize the Admin and Login Window" on page 249 for more information aboutcustomizing the email message sent to users when they

try to retrieve their username(s).

- Use the **Send email notification to users when password is changed** option to send an automated email after users reset their Privileged Access Service password via the forgot password process.
- Use the **Additional Attributes for MFA** options to configure additional attributes (such as other mobile phone, other home phone, other office phoneand other email addresses) for multi factor authentication (MFA). See"Configuring Additional Attributes for MFA" below.
- Use the **Specify trusted DNS domains for API calls** option to specify trusted domain names (for example your company domain, internet serviceprovide domains like AT&T, etc.) that can make calls to Privileged AccessService APIs. If calls are made from domains not listed here, the call will fail.

Configuring Additional Attributes for MFA

When you define the attributes using the **Additional Attributes for MFA** options, Privileged Access Service maps these additional attributes to Admin Portal and uses their values for MFA notification.

To add attributes:

1. Log in to Admin Portal.
2. Click **Settings > Authentication > Security Settings > Add** button in the Additional Attributes for MFA area.
3. Select an attribute from the drop-down list.

   Use the **Custom** attribute for other phone numbers, such as fax or IP phone. When you use the **Custom** attribute, the attribute name must matchone in the Attr LDAP Name column as shownhere.
4. Provide the relevant information based on the selected attribute.
5. Click **Add**.

   The attribute is added to the associated table.
6. Click **Save**.

We import all Active Directory user attributes, but we only monitor and accept updates for the attributes listed in the following table.

Attributes	Attributes	Attributes
accountExpires	lockoutTime	otherMobile
c	mail	pager
cn	manager	primaryGroupID

Attributes	Attributes	Attributes
co	member	postalCode
countryCode	memberOf	postOfficeBox
directReports	mobile	pwdlastset
distinguishedName	name	sAMAccountName
displayName	otherPager	sn
givenName	otherTelephone	st
groupType	otherMailbox	streetAddress
homePhone	otherFacsimileTelephoneNumber	userAccountControl
I	otherHomePhone	userPrincipalName
ipPhone	otherIpPhone	telephoneNumber
		wWWHomePage

The following table lists the Active Directory user attributes used by Office 365. Some of these attributes are duplicated in the above table.

Attributes	Attributes	Attributes
assistant	msExchArchiveName	msExchSenderHintTranslations
authOrig	msExchAssistantName	msExchTeamMailboxExpiration
c	msExchAuditAdmin	msExchTeamMailboxSharePoint Url
cn	msExchAuditDelegate	msExchUsageLocation
co	msExchAuditDelegateAdmin	msExchUserHoldPolicies
company	msExchAuditOwner	msRtcSip-ApplicationOptions
countryCode	msExchBlockedSendersHash	msRtcSip-DeploymentLocator
department	msExchBypassAudit	msRtcSip-Line
description	msExchBypassModerationFromDLMembers Link	msRtcSip-OptionFlags
displayName	msExchBypassModerationLink	msRtcSip-OwnerUrn
dLMemRejectPerms	msExchDelegateListLink	msRtcSip-PrimaryUserAddress
dLMemSubmitPerms	msExchElcExpirySuspensionEnd	msRtcSip-UserEnabled

Attributes	Attributes	Attributes
extensionAttribute1	msExchElcExpirySuspensionStart	objectGUID
extensionAttribute2	msExchElcMailboxFlags	objectSid
extensionAttribute3	msExchEnableModeration	otherFacsimileTelephoneNumber
extensionAttribute4	msExchExtensionCustomAttribute1	otherHomePhone
extensionAttribute5	msExchExtensionCustomAttribute2	otherIPPhone
extensionAttribute6	msExchExtensionCustomAttribute3	otherMobile
extensionAttribute7	msExchExtensionCustomAttribute4	otherPager
extensionAttribute8	msExchExtensionCustomAttribute5	otherTelephone
extensionAttribute9	msExchHideFromAddressLists	pager
extensionAttribute10	msExchImmutableId	physicalDeliveryOfficeName
extensionAttribute11	msExchLitigationHoldDate	postalCode
extensionAttribute12	msExchLitigationHoldOwner	postOfficeBox
extensionAttribute13	msExchMailboxAuditEnable	preferredLanguage
extensionAttribute14	msExchMailboxAuditLogAgeLimit	proxyaddresses
extensionAttribute15	msExchMailboxGuid	publicDelegates
facsimileTelephoneNumber	msExchModeratedByLink	pwdLastSet
givenName	msExchModerationFlags	samaaccountname
homePhone	msExchRecipientDisplayType	sn
info	msExchRecipientTypeDetails	st
initials	msExchRemoteRecipientType	streetAddress
IPPhone	msExchRequireAuthToSendTo	targetAddress
legacyExchangeDN	msExchResourceCapacity	telephoneAssistant
mail	msExchResourceDisplay	telephoneNumber
manager	msExchResourceMetadata	thumbnailPhoto
middleName	msExchResourceSearchProperties	title

Attributes	Attributes	Attributes
mobile	msExchRetentionComment	userAccountControl
msDS-HABSeniorityIndex	msExchRetentionURL	userCertificate
msDS-PhoneticDisplayName	msExchSafeRecipientsHash	userSMIMECertificate
msExchArchiveGuid	msExchSafeSendersHash	wWWHomePage

Remember Last Used Authentication Method

You can configure for Privileged Access Service to remember the most recent authentication method users used and present them with that method automatically. Users still have the option to select other configured authentication methods. For example, if you have configured email confirmation code and security question as the MFA methods and a user most recently answered a security question to authenticate into Privileged Access Service, then next time this user logs in to Privileged Access Service they will be presented with the security question automatically without needing to select it from the drop-down list.

Note: Android devices do not remember the last used authentication method after enrolling with MFA, but do remember the last used authentication method after launching an app or changing the password.

To remember the last used authentication method:

1. Log in to Admin Portal.
2. Click **Core Services** > **Policies** and select the policy you want to edit or click **Add Policy Set** to create a new one.
3. Click Authentication **Policies** > **Centrify Services**.
4. Enable the checkbox associated with the **Remember and suggest last used authentication factor** option.
5. Click **Save**.

How to Manage Tenant Signing Certificates

This scenario is intended to guide system administrators on how to add and manage signing certificates that are used to establish a secure connection between the Privileged Access Service and web applications. The Settings > Authentication > Signing Certificates page lists all of the certificates that have been uploaded to the Delinea tenant. In addition to uploading new certificates, you can also manage the existing set of certificates.

This scenario includes information on the following topics:

- Adding a Signing Certificate
- Viewing Signing Certificate Information
- Deleting a Signing Certificate
- Renaming a Signing Certificate

- odwnloading a Signing Certificate
- Setting a Signing Certificate as the Default
- Updating a Deprecated Signing Certificate

Adding a Signing Certificate

Before you deploy applications from the Delinea App Catalog, you can upload signing certificates to the Delinea tenant. The signing certificates can then be applied on a per-application basis when adding and configuring applications from the App Catalog.

Note: The Default Tenant Application Certificate displayed in the Signing Certificate page is set as the default. Most applications can be configured using the default tenant signing certificate. For more information on certificates and deploying applications, see "Applications" on page 823.

To add a new signing certificate:

1. In the Admin Portal, click Settings > Authentication > Signing Certificates to display the Signing Certificates page.
2. Click Add.
3. Type a name for the certificate and, if the file requires it, the password for the file.
4. Click Browse to upload an archive certificate file.
   - Make sure the certificate file is located on your local storage so you can select to upload it to the Delinea tenant.
5. Click Save.

Viewing Signing Certificate Information

Once the certificate file is uploaded it is displayed in the Signing Certificate page. The following information is displayed:

Field	Description
Name	The name given to the certificate file when it is was added to the Delinea tenant.
Default	A check mark indicates that the certificate is set as the default.
Subject	The organization name that issued the certificate.
Thumbprint	A unique string that identifies the certificate.
Algorithm	The cryptographic algorithm used in the certificate (such as SHA256RSA).

Field	Description
Issued By	The name of the Certificate Authority that issued the certificate.
Expires	The date when the certificate is no longer valid.
Uploaded	Yes indicates that the certificate was uploaded by the Delinea tenant. Blank indicates that the certificate is the default tenant signing certificate.

Deleting a Signing Certificate

You can remove a signing certificate from the Delinea tenant only if the certificate is not being used by an application, is uploaded by the tenant, and is not currently the default signing certificate (Default Tenant Application Certificate). If you try to remove a certificate that is in use, an error message is displayed and you are prevented from removing the certificate.

To remove a signing certificate from the Delinea tenant:

1. In the Admin Portal, click Settings > Authentication > Signing Certificates to display the Signing Certificates page.
2. Select the certificate that you want to delete from the list.
3. Click the Actions menu, then click Delete.
4. Click Yes to confirm that you want to proceed with deleting the certificate.

Renaming a Signing Certificate

If you need to change the name of a certificate you already uploaded, you can change it from the Signing Certificate page.

Note: The Default Tenant Application Certificate cannot be renamed.

To rename a signing certificate:

1. In the Admin Portal, click Settings > Authentication > Signing Certificates to display the Signing Certificates page.
2. Select the certificate that you want to rename.
3. Click the Actions menu, then click Rename.
4. Type the new name and then click Save.

Downloading a Signing Certificate

Any signing certificates uploaded to the Delinea tenant can be downloaded to your local computer or a destination you specify and used to configure applications from the App Catalog.

To download a signing certificate:

1. In the Admin Portal, click Settings > Authentication > Signing Certificates to display the Signing Certificates page.
2. Select the certificate that you want to download.
3. Click the Actions menu, then click Download.

Setting a Signing Certificate as the Default

The first time you log in to the Admin Portal the Default Tenant Signing Certificate is available and is set as the default signing certificate. If you upload additional signing certificates, you can change the signing certificate that you want to act as the default. The new signing certificate that you set as the default is then automatically used when you deploy applications unless you change it during the application configuration process.

To set a new default signing certificate:

1. In the Admin Portal, click Settings > Authentication > Signing Certificates to display the Signing Certificates page.
2. Select the certificate that you want to set as the default.
3. Click the Actions menu, then click Set as Default.

Updating a Deprecated Signing Certificate

Some applications have deprecated support for the SHA-1 signing certificate. If an application was deployed with a SHA-1 certificate that is now deprecated, and user authentication to the application fails, you need to update the security certificate. You can download the default SHA-2 certificate (Default Tenant Application Certificate) available from the Admin Portal or you can upload your own SHA-2 certificate and reapply it.

To update an expired signing certificate:

1. Download the default signing certificate from Settings > Authentication > Platform > Signing Certificates to your local computer. See Downloading a Signing Certificate for more information.

- Alternatively, you can upload your own SHA-2 certificate from Settings > Authentication > Signing Certificates and then click Add. See Adding a Signing Certificate for more information.

2. Apply the signing certificate for the application to Application Settings in the Admin Portal and to the application itself.

- Check the application documentation for details on how to apply the certificate to the application.

Note: Be sure to use a matching certificate both in the application settings in the Admin Portal and in the application itself.

Managing Certificate Authorities

A certificate authority (CA) is a trusted entity that issues digital certificates that verify a digital entity's identity. Digital certificates are an integral part of secure communication and play an important part in the public key infrastructure (PKI). Certificates typically include the public key, the expiration date of the certificate, the owner's name and other information about the certificate owner. Operating systems (OSes) and browsers maintain lists of trusted CA root certificates to verify the identity and validity of certificates that a CA has issued and signed. Certificate Authorities are enabled by the System Administrator.

To add a certificate

1. Click the **Add** button on the **Trusted Certificate Authorities** page. The **Trusted Certificate Authorities** window appears.
2. Add a name for your certificate by entering a name. Decide how you want the user login extracted and select from:
   - Principal Name from Subject Alternate Name
   - RFC 822 Name Subject Alternate Name
   - User Name from Subject
3. Choose the CA Chain by selecting the **Browse** button and selecting the certificate chain.

   Note: The uploaded file must contain all certificates required to establish chain trust from a user certificate. If chain trust verification requires intermediate authorities, package all required certificates in p7b format, and upload the p7b file. The p7b file should contain all intermediate authorities chaining up to a root authority.
4. Click **Save**.

To edit a certificate

1. Select the certificate you wish to edit, click the **Actions** button, and drill-down to select **Modify**.
2. The **Trusted Certificate Authorities** window appears. Edit the fields that you want to change.
3. Click **Save**.

To delete a certificate

1. Choose the certificate you want to delete, click the **Actions** button, and drill-down to select **Delete**.
2. A window appears asking if you are sure you want to delete the certificate. Click **Yes** and delete the certificate.

How to Configure Integrated Windows Authentication

Privileged Access Service lets you accept an Integrated Windows authentication (IWA) connection as sufficient authentication for users with Active Directory accounts when they log in to the Delinea portals. Privileged Access Service uses Kerberos SSO for authentication. With IWA enabled, the browser uses the current user's Active Directory information to prove its knowledge of the password through a cryptographic exchange with the in-process web server built into the connector. IWA is not available to Privileged Access Service account users.

If you have multiple connectors enabled for IWA, Privileged Access Service prioritizes connection with the connectors in the following order:

1. Connectors from the same IP address as the user's client machine.
2. Randomly chooses a connector if more than one is from the same IP address as the user's client machine. Multiple machines inside your network may appear as the same IP externally.
3. Chooses the best subnet match.
4. Randomly chooses a connector if none of the above are available.

To use IWA, users must be inside the external corporate IP range and specify their tenant URL in the portal URL in the following form:

- Admin Portal: `https://\<companyName\>.centrify.com/manage?customerID=ABC1234`

Prerequisites

Before you start configuring IWA with Privileged Access Service, make sure you have done the following:

- Relevant browsers are configured for IWA. See "How to Configure Browsers for Silent Authentication" on page 313.
- Specify an external corporate IP range using Admin Portal. See "How to Set Corporate IP Ranges" on page 318. Corporate IP range for IWA is for the external network only.
- Your company has at least 1 Delinea connector with web server enabled and that connector must be joined to Active Directory in the forest to which users are authenticating. See "Enabling IWA Service on the Connector" below.
- Decide if you want to use the Delinea tenant CA (recommended because the CA automatically installs to the Delinea connector and minimizes configurationsteps during roll-out), third-party CA (such as Symantec, GoDaddy, and so forth), or your internal CA.

Enabling IWA Service on the Connector

Integrated Windows authentication (IWA) is enabled by default when you install the connector. However, you may want to make configuration changes (for example, defining your corporate IP range) and ensure that browsers used by your users are configured properly for IWA. See "How to Configure Browsers for Silent Authentication" on page 313.

Note: You must restart the Delinea Connector after importing the certificate.

To configure IWA and import the certificate:

1. Log in to Admin Portal.
2. Click **Settings > Network > Centrify Connectors**.
3. Select the relevant connector or add a new one.

   You can modify the following settings:

Setting or property	Change to do the following
Enable web server	The default value is Enabled. This setting supports Integrated Windows Authentication and Office clients. If you disable the web server, you cannot change the DNS Hostname, HTTP Port Number and HTTPS Port number values.
DNS Hostname	The default is the connector's host computer's name. You can enter a DNS short name here or the fully qualified domain name in the IE local intranet zone.
IWA Detection Timeout	The length of time Integrated Windows Authentication (IWA) will wait for response from the connector. The default is 10 seconds.
HTTP Port Number	The default port is 80. Port 80 is the standard port. If you change the port number to a non-standard number (for example, 111), Firefox and Chrome may require additional configuration because these browsers block some non-standard ports. Do not change the port number unless you know the implications.
HTTPS Port Number	The default port is 8443. Port 8443 is the standard port. If you change the port number to a non-standard number, Firefox and Chrome may require additional configuration because these browsers block some non-standard ports. Do not change the port number unless you know about the implications.
Connector Host Certificate	The host certificate used by the Delinea Connector must be issued by a trusted issuer. You can trust the tenant specific CA we have created for you by default, or provide your own. Click **Upload** to upload a certificate into the Privileged Access Service. See Configuring SSL for certificate requirement information. Click **Download** to download your connector host certificate. Click **Download your IWA root CA certificate** to save a copy of the certificate from the IWA root CA.

1. Click **Save**.
2. Click **Corporate IP Range**.
3. Click **Add** to enter a your corporate IP range.

   IWA will not work for users whose computers are outside of the defined corporate IP range.
4. Click **OK**.
5. Reboot your Delinea Connector if you have uploaded a certificate.

Importing a Certificate

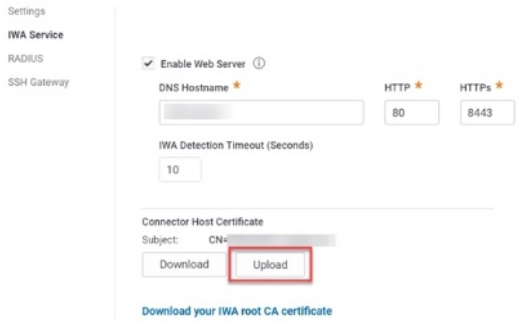
If you are using internal or third-party CAs (certificate authorities), you need to import those certificates into Privileged Access Service. You can import wildcard certificates.

For details about generating a certificate for the connector system, see Creating a connector machine certificate from an internal Microsoft CA.

To import a certificate into Privileged Access Service:

1. In the Admin Portal, go to **Settings > Network > Centrify Connectors**.
2. Select the relevant connector.
3. Click **IWA Service** on the Delinea Connector Configuration page.
4. Confirm that the **Enable Web Server** check box is enabled.
5. Click the **Upload** button to import an internal or third-party certificate.

   You can upload the same certificate to all Delinea Connectors in the same domain. If you do this, make sure you upload the same certificate to all IWA configured connectors.



6. Navigate to your CA and upload it.
7. Click **Save**.

Verifying IWA Over HTTPS

You can test the validity of the Delinea Connector host certificate by doing the following:

1. Open a web browser from an endpoint machine.
2. Navigate to the following address: `https://\<yourconnectorhostname\>:\<httpsport\>/iwa/ping`.

   Replace `\<YourConnectorHostname\>` and `\<httpsport\>` with the corresponding values. For example: `https://2008WindowsServer:8443/iwa/ping`
3. Look for the green certificate in the browser.

Enabling IWA in the Authentication Policy

You can configure Privileged Access Service to bypass already configured authentication rules and default authentication profiles when IWA is configured. This option is configured by default.

To enable IWA in the authentication policy:

1. Log in to Admin Portal.
2. Click **Access > Policies** and select the relevant policy set.

3. Click **Login Policies > Centrify Services**.
4. Click the **Enable authentication policy controls** drop-down and select **Yes**.
5. Select a default authentication profile (in the **Default Profile**dropdown) for Privileged Access Service to use if IWA is not available and other authentication conditions are not met.

   See "Creating Authentication Profiles" on page 284 for more information on authentication profiles.
6. Enable the **Allow IWA connections** option (enabled by default) in the “Other Settings” area.
7. Click **Save**.

Using IWA with Identity Cookie

This is an optional configuration. When you enable Integrated Windows Authentication (IWA), Privileged Access Service can write a cookie in the current browser after a successful IWA-based log in. Privileged Access Service checks the browser for this cookie when the user logs in to the Admin Portal. As long as the cookie is there, the user is not prompted for multi-factor authentication.

To use IWA with identity cookie:

1. Open the relevant Login Policy (**Login Policies > Centrify Services**).
2. Enable the **Set identity cookie for IWA connections** option in the “Other Settings” area.

   This option tells Privileged Access Service to write a cookie in the current browser after a successful IWA-based log in.
3. Click **Save**.

Using IWA to Authenticate Application Access

This is an optional configuration. You can configure Privileged Access Service to use IWA to override all application specific authentication requirements. For example, you can configure the Box application to require two authentication challenges if users are accessing the application from inside the network. However, you can tell Privileged Access Service to ignore those authentication requirements if IWA is available.

To allow IWA for applications that require authentication:

1. Open the relevant Login Policy (**Login Policies > Centrify Services**).
2. Enable the **IWA connections satisfy all MFA mechanisms** option.
3. This option tells the Privileged Access Service to allow IWA to override all application specific authentication requirements.
4. Click **Save**.

Disabling IWA

IWA is not required for manual authentication using Privileged Access Service. If you cannot use IWA on the corporate network, you can disable it.

To disable Integrated Windows authentication:

1. Log in to Admin Portal
2. Click **Settings > Network > Centrify Connectors**.
3. Select the relevant connector.
4. Unselect the **Enable Web Server** option.
5. Click **OK**.

How to Configure Integrated Windows Authentication

Privileged Access Service lets you accept an Integrated Windows authentication (IWA) connection as sufficient authentication for users with Active Directory accounts when they log in to the Delinea portals. Privileged Access Service uses Kerberos SSO for authentication. With IWA enabled, the browser uses the current user's Active Directory information to prove its knowledge of the password through a cryptographic exchange with the in-process web server built into the connector. IWA is not available to Privileged Access Service account users.

If you have multiple connectors enabled for IWA, Privileged Access Service prioritizes connection with the connectors in the following order:

1. Connectors from the same IP address as the user's client machine
2. Randomly chooses a connector if more than one is from the same IP address as the user's client machine. Multiple machines inside your network may appear as the same IP externally.
3. Chooses the best subnet match
4. Randomly chooses a connector if none of the above are available

To use IWA, users must be inside the external corporate IP range and specify their tenant URL in the portal URL in the following form:

- Admin Portal: https://<companyName>.centrify.com/manage?customerID=ABC1234

Prerequisites

Before you start configuring IWA with Privileged Access Service, make sure you have done the following:

- Relevant browsers are configured for IWA. See [How to Configure Browsers for "How to Configure Browsers for Silent Authentication" on page 313.
- Specify an external corporate IP range using Admin Portal. "How to Set Corporate IP Ranges" on page 318. Corporate IP range for IWA is for the external network only.
- Your company has at least 1 Delinea connector with web server enabled and that connector must be joined to Active Directory in the forest to which users are authenticating. See "Enabling IWA Service on the Connector" on page 305.
- Decide if you want to use the Delinea tenant CA (recommended because the CA automatically installs to the Delinea connector and minimizes configurationsteps during roll-out), third-party CA (such as Symantec, GoDaddy, and so forth), or your internal CA.

Enabling IWA Service on the Connector

Integrated Windows authentication (IWA) is enabled by default when you install the connector. However, you may want to make configuration changes (for example, defining your corporate IP range) and ensure that browsers used by your users are configured properly for IWA. See "How to Configure Browsers for Silent Authentication" on page 313.

Note: You must restart the Delinea Connector after importing the certificate.

To configure IWA and import the certificate:

1. Log in to Admin Portal.
2. Click **Settings > Network > Centrify Connectors**.
3. Select the relevant connector or add a new one.

   You can modify the following settings:

Setting or property	Change to do the following
Enable web server	The default value is Enabled. This setting supports Integrated Windows Authentication and Office clients. If you disable the web server, you cannot change the DNS Hostname, HTTP Port Number and HTTPS Port number values.
DNS Hostname	The default is the connector's host computer's name. You can enter a DNS short name here or the fully qualified domain name in the IE local intranet zone.
IWA Detection Timeout	The length of time Integrated Windows Authentication (IWA) will wait for response from the connector. The default is 10 seconds.
HTTP Port Number	The default port is 80. Port 80 is the standard port. If you change the port number to a non-standard number (for example, 111), Firefox and Chrome may require additional configuration because these browsers block some non-standard ports. Do not change the port number unless you know the implications.
HTTPS Port Number	The default port is 8443. Port 8443 is the standard port. If you change the port number to a non-standard number, Firefox and Chrome may require additional configuration because these browsers block some non-standard ports. Do not change the port number unless you know about the implications.
Connector Host Certificate	The host certificate used by the Delinea Connector must be issued by a trusted issuer. You can trust the tenant specific CA we have created for you by default, or provide your own. Click **Upload** to upload a certificate into the Privileged Access Service. See [Configuring SSL for certificate requirement information]. Click **Download** to download your connector host certificate. Click **Download your IWA root CA certificate** to save a copy of the certificate from the IWA root CA.

1. Click **Save**.
2. Click **Corporate IP Range**.
3. Click **Add** to enter a your corporate IP range.

   IWA will not work for users whose computers are outside of the defined corporate IP range.
4. Click **OK**.
5. Reboot your Delinea Connector if you have uploaded a certificate.

Importing a Certificate

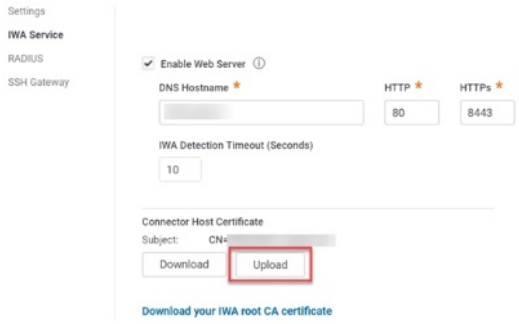
If you are using internal or third-party CAs (certificate authorities), you need to import those certificates into Privileged Access Service. You can import wildcard certificates.

For details about generating a certificate for the connector system, see Creating a connector machine certificate from an internal Microsoft CA

To import a certificate into Privileged Access Service:

1. In the Admin Portal, go to **Settings > Network > Centrify Connectors**.
2. Select the relevant connector.
3. Click **IWA Service** on the Delinea Connector Configuration page.
4. Confirm that the **Enable Web Server** check box is enabled.
5. Click the **Upload** button to import an internal or third-party certificate.

   You can upload the same certificate to all Delinea Connectors in the same domain. If you do this, make sure you upload the same certificate to all IWA configured connectors.



6. Navigate to your CA and upload it.
7. Click **Save**.

Verifying IWA Over HTTPS

You can test the validity of the Delinea Connector host certificate by doing the following:

1. Open a web browser from an endpoint machine
2. Navigate to the following address: https://<yourconnectorhostname>:<httpsport>/iwa/ping.

Replace <YourConnectorHostname> and <httpsport> with the corresponding values. For example: https://2008WindowsServer:8443/iwa/ping

3. Look for the green certificate in the browser.

Enabling IWA in the Authentication Policy

You can configure Privileged Access Service to bypass already configured authentication rules and default authentication profiles when IWA is configured. This option is configured by default.

To enable IWA in the authentication policy:

1. Log in to Admin Portal.
2. Click **Access > Policies** and select the relevant policy set.
3. Click **Login Policies > Centrify Services**.
4. Click the **Enable authentication policy controls** drop-down and select **Yes**.
5. Select a default authentication profile (in the **Default Profile**dropdown) for Privileged Access Service to use if IWA is not available and other authentication conditions are not met.

   See "Creating Authentication Profiles" on page 284 for more information on authentication profiles.
6. Enable the **Allow IWA connections** option (enabled by default) in the “Other Settings” area.
7. Click **Save**.

Using IWA with Identity Cookie

This is an optional configuration. When you enable Integrated Windows Authentication (IWA), Privileged Access Service can write a cookie in the current browser after a successful IWA-based log in. Privileged Access Service checks the browser for this cookie when the user logs in to the Admin Portal. As long as the cookie is there, the user is not prompted for multi-factor authentication.

To use IWA with identity cookie:

1. Open the relevant Login Policy (**Login Policies > Centrify Services**).
2. Enable the **Set identity cookie for IWA connections** option in the “Other Settings” area.

   This option tells Privileged Access Service to write a cookie in the current browser after a successful IWA-based log in.
3. Click **Save**.

Using IWA to Authenticate Application Access

This is an optional configuration. You can configure Privileged Access Service to use IWA to override all application specific authentication requirements. For example, you can configure the Box application to require two

authentication challenges if users are accessing the application from inside the network. However, you can tell Privileged Access Service to ignore those authentication requirements if IWA is available.

To allow IWA for applications that require authentication:

1. Open the relevant Login Policy (**Login Policies > Centrify Services**).
2. Enable the **IWA connections satisfy all MFA mechanisms** option.
3. This option tells the Privileged Access Service to allow IWA to override all application specific authentication requirements.
4. Click **Save**.

Disabling IWA

IWA is not required for manual authentication using Privileged Access Service. If you cannot use IWA on the corporate network, you can disable it.

To disable Integrated Windows authentication:

1. Log in to Admin Portal
2. Click **Settings > Network > Centrify Connectors**.
3. Select the relevant connector.
4. Unselect the **Enable Web Server** option.
5. Click **OK**.

How to Configure Browsers for Silent Authentication

Silent authentication applies to Integrated Windows Authentication (IWA) and certain RADIUS authentication methods. For silent authentication to work when logging in to the Privileged Access Service Admin Portal, a few browser configuration tasks may be necessary.

- **Firefox**: Either set `network.negotiate-auth.allow-non-fqdn` to True or add the connector host name to the `network.negotiate-auth.trusted-uris` list of trusted sites (see "Configuring Firefox to Allow Silent Authentication" on the next page.
- **Internet Explorer**: Make sure Integrated Windows Authentication (IWA) is enabled, and then in most cases silent authentication works without further configuration. Additional details are included here in case you need to make some configuration changes (see "Configuring Internet Explorer Security Zones" on page 315.
- **Safari**: In most cases, silent authentication works without further configuration. Additional details are included here in case you need to make some configuration changes (see "Configuring Google Chrome on Windows for Silent Authentication" on page 318 or "Configuring Apple Safari on a Mac for silent authentication" on page 318.
- **Chrome** and **Safari**: In most cases, silent authentication works without further configuration. Additional details are included here in case you need to make some configuration changes (see "Configuring Google Chrome on Windows for Silent Authentication" on page 318.

  Note: Silent authentication works as installed with Windows Firewall. If you are using a different firewall system, be sure to allow traffic on the port specified in Delinea Connectors in Settings in Admin Portal. By default, this port is 80.

Configuring Firefox to Allow Silent Authentication

To enable silent authentication for users logging in to the Privileged Access Service Admin Portal, you must import the tenant root CA to the browser and do one of the following in the users' browser:

- If you did not change the connector host name to a fully qualified domain name (by default it is not), you set the`network.negotiate-auth.allow-non-fqdn` Preference Name to **true**.

  Note: By default, the host name used by Privileged Access Service uses the format of http://*hostname*, where hostname is the host name of the connector.

- If you did change the connector host name to a fully qualified domain name, you need to add the fully qualified domain names for the connector host computers to the `network.negotiate-auth.trusted-uris` Preference Name.

  You can add the fully qualified domain names as a –for example, mycompany.com (do not enter a character)–or list each one individually. Listing them individually is more secure. However, you must remember to add the fully qualified domain name every time you add a new connector host.

To configure silent authentication in Firefox using`network.negotiate-auth.allows-non-fqdn**:**`

1. Open Firefox.
2. Type about:config as the target URL.
3. Type neg in the Filter field.
4. Select `network.negotiate-auth.allow-non-fqdn`. If it is set to **false**, right-click and select **Toggle**. If it is already set to true, do not change it.
5. Close the about:config tab and close Firefox.

To configure silent authentication in Firefox using`network.negotiate-auth.trusted-uris**:**`

1. Open Firefox.
2. Type about:config as the target URL.
3. Type neg in the Filter field.
4. Select and right click `network.negotiate-auth.trusted-uris` and select **Modify**. Enter a comma-separated list of the fully qualified domain name for each connector as string values, then click **OK**.

   For example, if you have two connectors–hosta.mycompany.com and hostb.mycompany.com–you click Modify, enter the following and click OK.

   `hosta.mycompany.com,hostb.mycompany.com`

   The less-secure alternative would be to enter just the domain name. For example, you would click Modify, enter the following and click **OK**.

   `smycompany.com`
5. Close the about:config tab and close Firefox.

Configuring Internet Explorer Security Zones

For users to be authenticated silently when they use Internet Explorer to open Privileged Access Service Admin Portal two conditions must be met:

- Internet Explorer must have integrated Windows authentication enabled. For details, see "Enabling Integrated Windows Authentication" below.
- If you are using a fully qualified domain name (FQDN) URL, the connector must be in the **local intranet** Internet Explorer security zone or explicitly configured as part of the local intranet security zone.

For Internet Explorer, a server is recognized as part of the local intranet security zone in one of two ways:

- When the user specifies a URL that is not a fully qualified DNS domain name. For example, if you access an application with a URL such ashttp://acme/index.html, Internet Explorer interprets this as a site in the local intranet security zone.

  Note: By default, the connector host name is not a fully qualified DNS domain name. Privileged Access Service uses the format of https://*hostname*, where hostname is the host name of the connector.

- When the user specifies a URL with fully qualified name that has been explicitly configured as a local intranet site in Internet Explorer (see instructions below). For example, if you access an application with a URL such as http://acme.mycompany.com/index.html, Internet Explorer interprets this as a site that is not part of the local intranet unless the site has been manually added to the local intranet security zone.

Depending on whether users log on to Web applications using a local intranet URL or a fully-qualified path in the URL, silent authentication may require modifying the local intranet security zone in Internet Explorer.

Enabling Integrated Windows Authentication

Use the following procedure to enable silent authentication on each computer.

To enable Integrated Windows Authentication for Internet Explorer:

1. Open Internet Explorer and select **Tools > Internet Options**.
2. Click the **Advanced** tab.
3. Scroll down to the **Security** settings.
4. Check the **Enable Integrated Windows Authentication** box.
5. Restart Internet Explorer.

Adding a Web Site to the Local Intranet Security Zone

By default, the Delinea Connector host name is not a fully qualified domain name. When this is the case, you do not need to add the URL – https://hostname – to the local intranet, and users get silent authentication when they log in to the Privileged Access Service Admin Portal.

However, if you change the connector host name to a fully qualified domain name, you need to add the connector host FQDN URL (https://hostname.domain.com) in each user's Internet Explorer Local Intranet before they can get silent authentication.

To add the connector host FQDN URL to the Internet Explorer local intranet:

1. Open Internet Explorer and select **Tools > Internet Options**
2. Click the **Security** tab.
3. Click the **Local intranet** icon.
4. Click **Sites**.
5. Click **Advanced**.
6. Type in the URL https://*hostname.domain.com* in the text box and click **Add**. Then click **Close**.

   Note: If there is a URL in the text box already, either delete it or click **Add** to save it.

7. Click **OK** to accept the local intranet configuration settings, then click **OK** to close the Internet Options dialog box.

Configuring Edge to Allow Silent Authentication

When using Microsoft Edge to open the Privileged Access Service Admin Portal, users can only be authenticated silently when the browser has integrated Windows authentication enabled. For details, see "Enabling Integrated Windows Authentication" on the previous page.

For Edge, a server is recognized as part of the local intranet security zone when the user specifies a URL with a fully qualified name that has been explicitly configured as a local intranet site in Edge (see instructions below). For example, if you access an application with a URL such as http://acme.mycompany.com/index.html, Edge interprets this as a site that is not part of the local intranet unless the site has been manually added to the local intranet security zone.

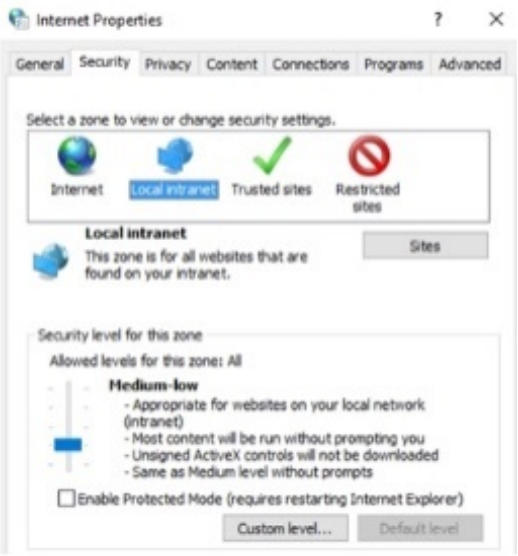
Enabling Integrated Windows Authentication

Use the following procedure to enable silent authentication on each computer.

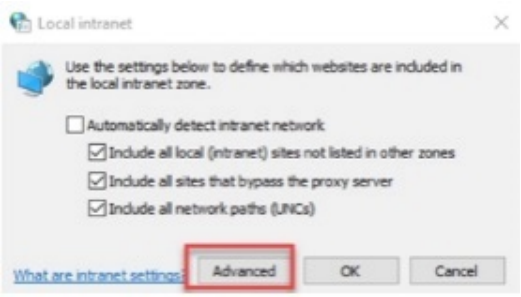
To enable Integrated Windows Authentication for Edge:

1. Open the Windows Settings and search **Internet Options**.

   The following window opens.



2. Click **Local intranet > Sites**.
3. Click **Advanced**.



4. Enter the tenant specific URL into the Websites text box.

5. Click **Close**.

Configuring Google Chrome on Windows for Silent Authentication

In most cases, silent authentication works for Google Chrome without additional configuration, if the connector host name is available in your DNS.

Configuring Google Chrome on a Mac for Silent Authentication

Google Chrome on Mac requires you to whitelist an authentication server to successfully authenticate your users.

To configure Chrome on a Mac for silent authentication and single sign-on

1. Log in to your Mac device as an Active Directory user.
2. Quit any instances of Chrome, then open the Terminal.
3. Run the following command in the Terminal.

```
defaults write com.google.Chrome AuthServerWhitelist \<connector hostname\>
```

Connector hostname is the hostname set in **Settings > Network > Delinea Connectors**.

Tip: If you have more than one connector configured, use a comma to separate the host names. For example:

```
defaults write com.google.Chrome AuthServerWhitelist host1,host2
```

Your users should now be able to use silent authentication with Chrome on a Mac. If the changes in the previous procedure do not take effect immediately, Quit Google Chrome and then force any remaining Google Chrome related process to quit using the Activity Monitor.

Configuring Apple Safari on a Mac for silent authentication

If you have a Server Suite Agent installed on a Mac, silent authentication automatically works in the Safari web browser. For more information about Delinea products on the Mac, see the *Administrator's Guide for Mac*.

How to Set Corporate IP Ranges

You use the Corporate IP Range feature to define IP ranges for your internal network and external network. Connections that are made from inside the corporate IP range have the following privileges:

- Active Directory users can log in to Admin Portal and the Privileged Access Service Admin Portal with silent authentication. (This requires Integrated Windows authentication – see "How to Configure Integrated Windows Authentication" on page 309.
- If you enable authentication policy controls, these users can be exempt from the additional authentication requirements.

These IP ranges are typically used to identify authentication requirements. For example, they can be used for Integration Windows authentication or multifactor authentication (see "Creating Authentication Rules" on page 281.

To specify external IP addresses for silent authentication and access control:

1. Log in to Admin Portal.
2. Click **Settings > Network > Corporate IP Range > Add**.
3. Enter a name to quickly identify the IP address or range.

4. Enter an IP address or a range of addresses in the form `\<network\>/\<subnet mask\>`.

   Admin Portal shows your current external IP address under the text box.

5. Click **OK**

Repeat to specify additional addresses or ranges.

Block IP Addresses From Accessing Privileged Access Service

You can block a specific IP address or a range of addresses from accessing Privileged Access Service.

To block the an IP address or range:

1. Log in to Admin Portal.
2. Click **Settings** > **Network** > **Blocked IP Ranges**.
3. Click the **Add** button.
4. Enter a name to identify the configuration.
5. Enter the IP address or range.

   Entering `11.222.33.44/5` means you are blocking the IP range of `.44 to .49`.

6. Click **OK**.

Temporarily Suspend Multifactor Authentication

If the user's account information required for multifactor authentication is not set properly and it prevents the user from logging in, you can use the MFA Unlock command in Admin Portal to suspend multifactor authentication for 10 minutes – see "User Management Commands" on page 274. The user must still enter the correct user name and password and is still prompted to enter the additional authentication factor, however, the Privileged Access Service

does not validate anything beyond the user name and password. Consequently, the user can, for example, enter any string of characters to fulfill the SMS confirmation code, and the Privileged Access Service accepts the entry.

To temporarily suspend multifactor authentication for a user:

1. Log in to Admin Portal.
2. Click **Access > Users**.
3. Right-click the account for the user who is locked out.
4. Select **MFA Unlock**.

   The user has 10 minutes to log in.

How to Set Up Smart Card Authentication

Smart card log in is a certificate-based log in. The certificate is supplied by the smart card and used by Privileged Access Service to authenticate users. To use smart card authentication with Privileged Access Service, your users must already be configured for smart card log in.

To set up smart card authentication:

1. Log in to the Admin Portal.
2. Click **Access > Policies**.
3. Select the relevant policy or create a new one.
4. Click **Authentication Policies > Centrify Services**.
5. Confirm that **Use certificates for authentication** (in the Other Settings section) is enabled (default).

   You must have this option enabled to use smart card authentication. This option allows Privileged Access Service to use the smart card generated certificate to authenticate users to the cloud.
6. (Optional) Enable the **Set identity cookie for connections using certificate authentication** option only if you have a hybrid system where users are logging in using smart cards and another authentication method.

   Enabling this option will allow the Privileged Access Service to write cookies in the browser after a successful log-in. Privileged Access Service will then check the browser for this cookie upon subsequent log ins and take action based on any identity cookie authentication rules you have configured. See "Creating Authentication Rules" on page 281.
7. Upload your certificate authority chain.
   a. Log-in to Admin Portal.
   b. Click **Settings > Authentication > Certificate Authorities**.
   c. Provide a unique name for the trusted certificate authority.
   d. Specify the field to use for extracting the user login name from the certificate.
   Select the same field for all certificates in the chain.
   e. Click **Browse** to select certificate authority chain for uploading.
   The uploaded chain must contain all certificates for chain validation, starting from intermediate CA trusting to a root certificate authority.

> **Note:** The uploaded file must contain all certificates required to establish chain trust from a user certificate. If chain trust verification requires intermediate authorities, package all required certificates in p7b format, and upload the p7b file. The p7b file should contain all intermediate authorities chaining up to a root authority.

f. (Optional) Select the **Enable Client Certificate Revocation Check**check box to allow Privileged Access Service to verify that the smart card certificate has not been revoked.
If the user certificate has revocation check information -- CRL Distribution Point (CDP) or Online Certificate Signing Protocol (OCSP)URL -- and the **Enable Client Certificate Revocation Check** option is enabled on the CA chain, Privileged Access Service communicates with the certificate endpoints to check for certificate validity.

Important: To perform certificate revocation checks, CDP URLs and OCSP URLs must be reachable from the Internet. Turning on revocation check on the CA chain when revocation check endpoints are not reachable from the Internet causes certificate authentication to fail.
This revocation check is specific to smart card logins. After derived credentials are securely stored on enrolled devices, this check does not impact the derived credentials.

g. Click **Save**.

For more information on managing certificate authorities, see "Managing Certificate Authorities" on page 304.

How to Enable FIDO2 Authentication

FIDO2 is an authentication standard hosted by FIDO Alliance. This standard includes the Web Authentication ("WebAuthn") API, which is a specification written by the World Wide Web Consortium (W3C) and FIDO, with participation from additional third parties. The WebAuthn API is backward compatible with Universal 2nd Factor (U2F) keys.

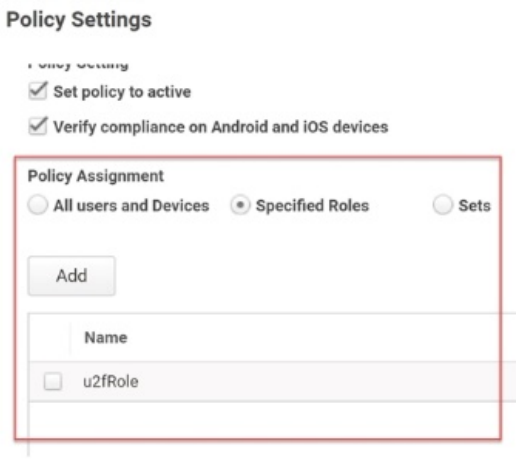
Delinea leverages the WebAuthn API to enable password less authentication to the Privileged Access Service using either on-device or external authenticators. On-device authenticators are biometric authenticators integrated into the device hardware. Popular examples are Mac Touch ID, Windows Hello, and fingerprint scanners. External authenticators are security keys that you plug into the device's USB port; for example, a YubiKey.

Refer to https://webauthn.io/ and https://fidoalliance.org/fido2/ for more information about WebAuthn and FIDO2, respectively.

To enable FIDO2 authentication for users:

1. Log in to Admin Portal.
2. Click **Access > Policies**.
3. Select a policy set or create a new one.
4. Specify the users/roles to which this policy applies using the **Policy Assignment** options.

   This configuration option is particularly important if you are creating a new policy.



5. Click **User Security Policies > User Account Settings**.
6. Select **Yes** in the **Enable users to register FIDO2 Authenticators** drop-down box.
7. Choose **Yes** or **No** in the **Require users to setup FIDO2 Authenticator on login** drop-down.
8. Enter a name in the **FIDO2 Security Key Display Name** field.

   This name should be recognizable by your users.
9. (Optional) Select an authentication profile to require users to provide additional authentication before they can activate and modify the FIDO2 Authenticator in the Admin Portal.

   See "Creating Authentication Profiles" on page 284 or information about authentication profiles.
10. Click **Save**.

Users can now log in to Admin Portal and activate their FIDO2 authenticator(s). You can direct users to "Using FIDO2 Authenticators" on page 367for activation instructions.

Using FIDO2 Authenticators with a New Tenant URL

FIDO2 authenticators are associated with the portal URL. If your company gets a new portal URL, because you configured a tenant URL or for another reason, then users with FIDO2 authenticators will need to log in with the new URL and re-activate their authenticators. Users who do not activate their authenticators on the new URL will not see their authenticator as an authentication option. For example, if you are changing the URL from `https://aad0123.my.abc.com` to `https://company.my.abc.com`, then users who authenticated to `https://aad0123.my.abc.com` using their FIDO2 authenticator must log into the new URL -- `https://company.my.abc.com` -- and activate their authenticator.

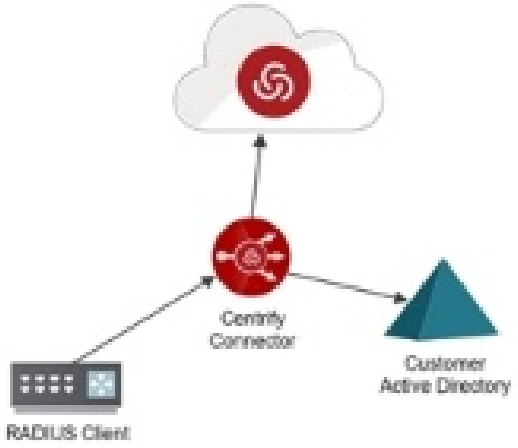
Verify the following to ensure a smooth transition for your users:

1. You have configured an alternative authentication mechanism for FIDO2 users so they can log in with the new URL and activate their FIDO2 authenticator(s). For example, if you have a role containing all your users with FIDO2 authenticator(s), then make sure the authentication profile associated with that role has email address or security questions enabled. See "Reference Content – Authentication" on page 356 for information about each authentication mechanism.

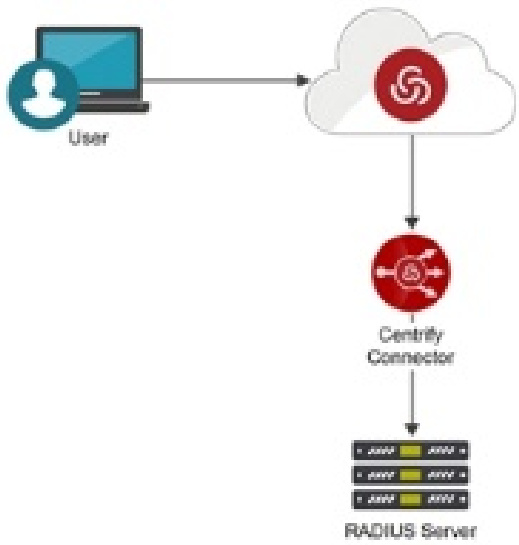
2. You have confirmed with the relevant users that they can log in to Privileged Access Service using the alternative authentication mechanisms and they have re-activated the FIDO2 authenticator(s). Instructions for users to activate their FIDO2 authenticator(s) are here: "Using FIDO2 Authenticators" on page 367.

How to Configure Privileged Access Service for RADIUS

Privileged Access Service supports RADIUS in two ways. The first is to use the Delinea Connector as a RADIUS server for clients that support RADIUS authentication, such as VPNs. Using Privileged Access Service with your RADIUS client, you can provide a second authentication layer for added security. For example, if a VPN concentrator uses RADIUS for authentication, you can configure email as a secondary authentication requirement. A typical work flow is when a RADIUS client (like a VPN server) uses the Delinea Connector as a RADIUS server to authenticate an incoming user connection. Depending on the user type, the connector authenticates the credentials either through Active Directory or Privileged Access Service and returns the authentication result to the RADIUS client. This diagram shows the work flow. See "Configuring the Delinea Connector for Use as a RADIUS Server" on the next page for configuration details.



The second way to use RADIUS with Delinea is to use your existing RADIUS server for user authentication into Privileged Access Service by defining the Delinea Connector as a RADIUS client. When users attempt to log in to Privileged Access Service and selects an external RADIUS server as a multi-factor authentication (MFA) mechanism, we send the user credentials (username and passcode) to the connector, which validates them against the configured RADIUS server, and returns the result of that validation to Privileged Access Service . This diagram shows the work flow. See "Configuring the Delinea Connector for Use as a RADIUS Client" on page 335 for configuration details.



Configuring the Delinea Connector for Use as a RADIUS Server

To enable communication between your RADIUS client and the connector (acting as a RADIUS server), do the following:

1. Make configuration changes in the Admin Portal to designate the connector as a RADIUS server, add the RADIUS client information, and define the requirement for a secondary authentication mechanism. See "Configuring the Admin Portal (connector as a RADIUS server)" below.
2. Configure the RADIUS client (for example Cisco VPN, Juniper VPN, and Palo Alto VPN). See "Setting Up a RADIUS Client" on page 329 for client configuration details.

Configuring the Admin Portal (connector as a RADIUS server)

Make configuration changes in the Admin Portal to designate the connector as a RADIUS server, define the RADIUS client information, and define the requirement for a secondary authentication mechanism.

To configure the Admin Portal:

1. Log in to the Admin Portal.
2. Configure the connector to be a RADIUS server.
   a. Click **Settings > Network > Centrify Connector**.
   b. Select an existing connector or add a new one.
   c. Click **RADIUS**.
   d. Select the **Enable incoming RADIUS connections** checkbox.

      Your VPN server and the connector must be able to communicate. Confirm with your network administrator that your corporate firewall rules arenot blocking this connection, for example if your VPN server is in the DMZ.

e. Provide the port number in which the Delinea Connector talks to Privileged Access Service. The default port number is 1812.

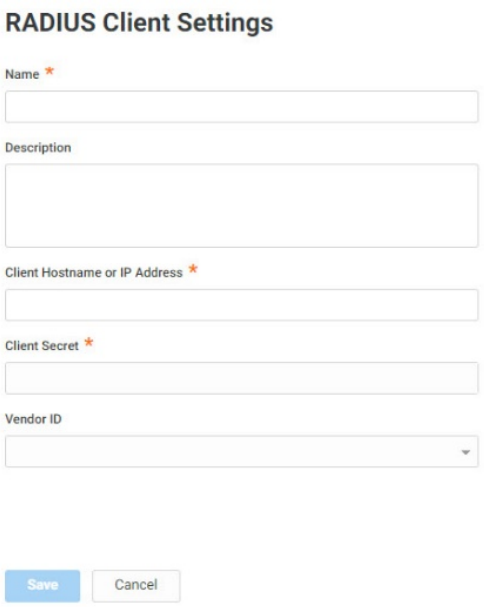
f. Click **Save**.

3. Define the RADIUS client information.

a. Click **Authentication > RADIUS Connections > Client** tab **> Add** to configure your RADIUS client.

A RADIUS client can be VPN server, wireless access point, etc.

b. Enter the required information.



The **Client Hostname or IP Address** field is expecting the hostname or IP address of the RADIUS client.

The **Client Secret** field is expecting a shared secret key for the RADIUS client and Privileged Access Service. If you have entered a secret key on your RADIUS client, then enter that same key here. The keys must match to enable authentication. If you are creating a new secret key, best practices recommend 22 or more characters in length.

(Optional) The **Vendor ID** field is used for defining custom RADIUS attributes and is expecting an integer identifier for your RADIUS vendor. Each vendor (Cisco, Juniper Networks, etc.) has unique IDs for their RADIUS Vendor-Specific Attributes (VSA). The drop-down list provides a few common VSAs, but you can also enter a vendor ID for your specific RADIUS VSA. When entering your vendor ID, only integers are accepted. The descriptive text associated with VSA in the drop-down list is ignored by our back-end system. See "Configuring the Admin Portal (connector as a RADIUS server)" on the previous page to configure the custom RADIUS attributes.

c. Click **Response**.

d. (Optional) Select the language in which RADIUS client messages and user communications (Email and SMS) will be displayed.

e. (Optional) The “Include new-line characters in the mechanism selection list prompt” option controls how the mechanism list is displayed. This image shows the list when this option is enabled.

This image shows the list when this option is disabled.

f. Specify the **Wait Timeout** (a time, in seconds, the service should wait for an out-of-band response).

g. Specify the user response option for each authentication mechanism. Select **Push** for users to respond from the mechanism (for example, click a link in the email or tap a link in the text message). Select**Enter Code** for users to manually enter the code on the RADIUS client UI.

h. Click **Save**.

4. Enable the RADIUS client connection and define the secondary authentication requirement.

   a. Click **Polices** and either select an existing policy set or add a new one.

   b. Click **User Security Policies > RADIUS**.

   c. Select **Yes** in the **Allow RADIUS client connections** dropdown.

      This setting allows users to authenticate with the RADIUS client.

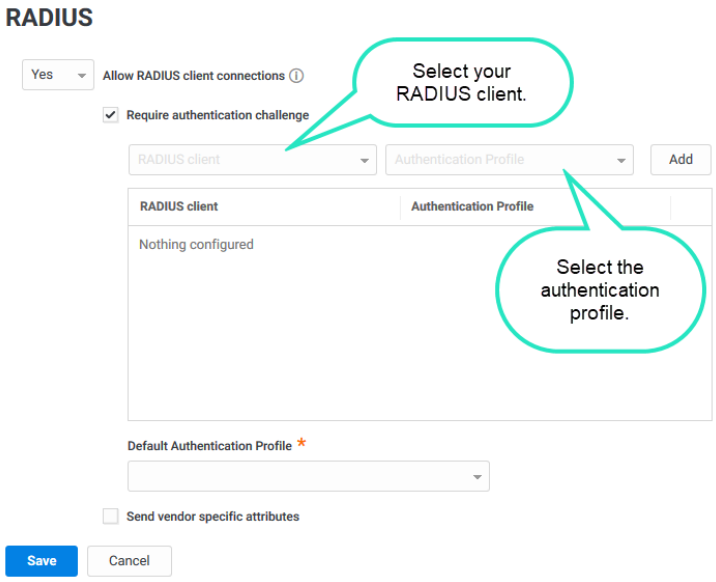
d. Select the **Require authentication challenge** check box to require that users provide a secondary authentication mechanism to log in via the RADIUS client.

e. (Optional) Configure an authentication profile for specific RADIUS clients.

   i. Click the **Add Authentication Profile** button.

   ii. Select the **RADIUS client** from the drop-down list.

   iii. Select an **Authentication Profile** from the drop-down list or **Add New Profile**.



Important: We recommend that the first challenge in the profile is Password because the user prompt from the RADIUS client defaults to Username/Password, regardless of the authentication mechanism (s)you choose for the first challenge. If your first challenge is not Password, for example it is Mobile Authenticator, then users may not successfully authenticate with the RADIUS client because we are expecting a mobile authenticator code but users enter their username/password based on the UI prompt.

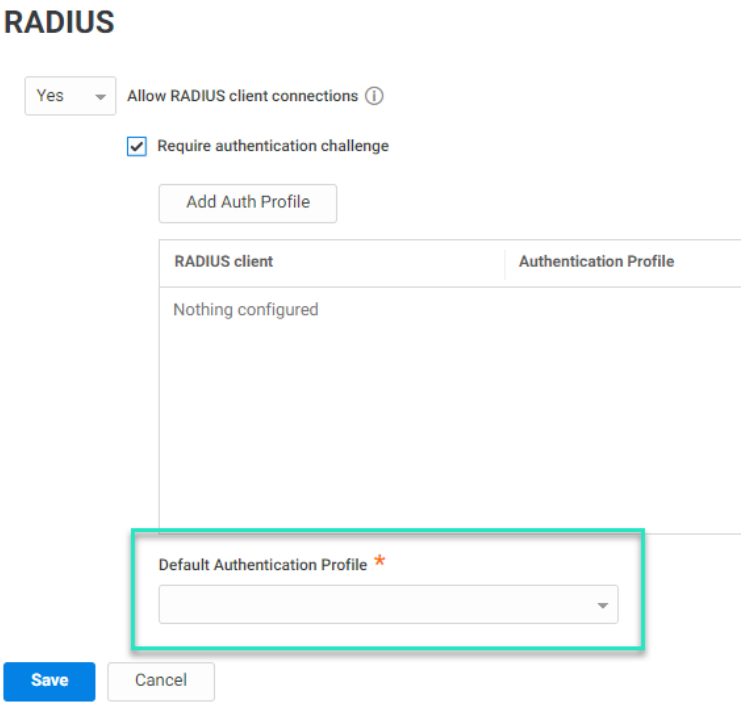
Verify that your RADIUS client allows for the selection of an authentication mechanism when multiple mechanisms are available. Some RADIUS clients do not support the selection of an authentication mechanism when more than one mechanism is available. Therefore, if your authentication profile has more than one mechanism in the second challenge, users will not be authenticated with some RADIUS clients.

See "Creating Authentication Profiles" on page 284 for information on authentication profiles.

   iv. Click the **Add** button.

f. Select an authentication profile from the **Default Authentication Profile** drop-down list to define authentication requirements for all your RADIUS clients or a profile to be used for any clients you did not specify in the above step.

For example, users coming in via a RADIUS client not specified above will be authenticated using the authentication profile selected here.



See "Creating Authentication Profiles" on page 284 for information on authentication profiles.

5. (Optional) Define custom RADIUS attributes for authentication response

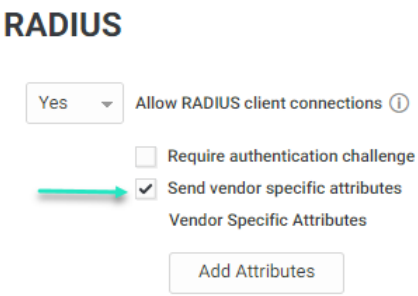
   You can define the RADIUS attributes sent to the RADIUS client. The RADIUS client can then interpret the attributes based on defined standards. For example, you can define a "contract employee" attribute and associate only contract/contingent workers to this Privileged Access Service policy; then you can configure the RADIUS client with a VPN access policy specifically for contract/contingent workers.

   a. Confirm that you have specified the Vendor ID when you configured your RADIUS client information in step 3.

   b. Click **Policies** and either select an existing policy set or add a new one.

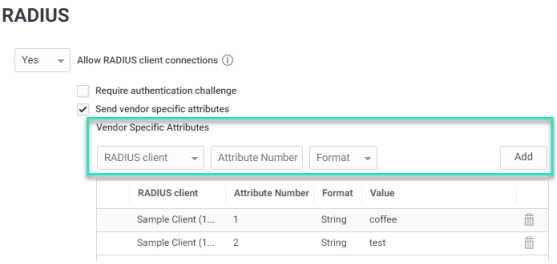
   c. Click **User Security Policies > RADIUS**.

   d. Select the **Send vendor specific attributes** check box.



   e. Click the **Add Attributes** button.

f. Specify the necessary information.



Select the relevant client from the **RADIUS client** dropdown list.

Enter the **Attribute Number**. This number identifies the attribute and must be a unique number. For example, if you have created an attribute with the number 2, you can not create another attribute using the same number.

Select the attribute **Format** -- string or integer.

Enter the attribute **Value**.

g. Click the **Add** button.

The newly created attribute is shown in the table.

h. Click **Save**

Setting Up a RADIUS Client

The steps for configuring a RADIUS client to work with the Delinea Connector vary for each client. Refer to your RADIUS client documentation for the configuration procedure and guidelines.

At a high level, you consistently need the following information regardless of the RADIUS client device:

- IP address of the Delinea Connector
- The secret key you provide to the RADIUS client and Admin Portal must match exactly

Important: For Open VPN, the Delinea Connector only supports the PAP authentication method.

To configure RADIUS authentication on a Cisco ASA device:

1. On the Cisco ASDM for ASA interface, create an IP Name object for the target by doing the following:
   a. Navigate to **Firewall**, expand **Objects**, and select **IP Names**.
   b. Click **Add** and enter a descriptive name (for example, Privileged Access Service RADIUS), the IP address of the Delinea Connector, and a description (for example, Privileged Access Service RADIUS Bridge).
   c. Click **OK** then **Apply**.
2. Create a AAA server group by doing the following:
   a. Click **Remote Access VPN**.
   b. Click **AAA Setup**, **AAA Server Group**, then **Add**.
   c. Enter a server group name, for example “Privileged Access Service"

d. Confirm that the RADIUS protocol is selected.

e. Accept the default for the other settings and click **OK**.

3. Add the RADIUS server to the server group by doing the following:

a. Select the newly created server group.

b. Click **Add**.

c. Under the Interface Name, select the interface on the ASA that will have access to the RADIUS server.

d. Under "Server Name or IP Address" enter the IP Name you created for the RADIUS server (i.e. DelineaRADIUS).

e. In the Server Secret Key field, enter the secret key that you entered in the Privileged Access Service Admin Portal interface.

f. In the Common Password field, re-enter the pass phrase/secret key.

g. Accept the default for the other settings and click **OK**.

To configure RADIUS authentication on a Juniper device:

1. Open the Juniper Secure Networks Secure Access SSL-VPN Central Manager.
2. Navigate to **Authentication** > **Authentication Servers** > **New Server**.

3. Provide the following information:

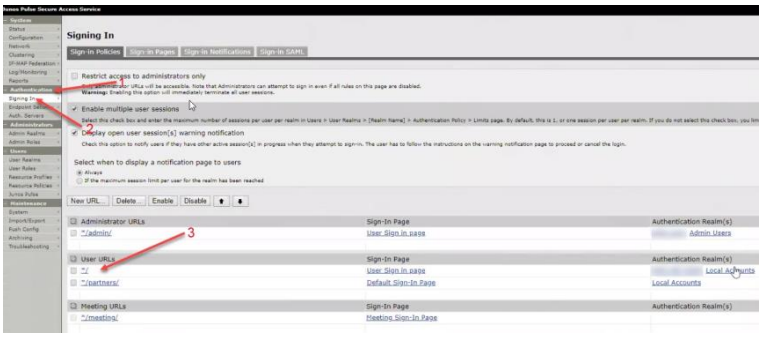
- Name: Descriptive name such as Delinea RADIUS.
- NAS-Identifier: Descriptive name such as Juniper.
- Radius Server: IP address of the Delinea Connector.
- Authentication port: 1812
- Shared Secret: The secret key that you entered in the Privileged Access Service Admin Portal interface.
- NAS-IP-Address: IP address of the Juniper device.
- Timeout: 30 seconds
- Retries: 0
- Users authenticate using tokens or one-time password: leave unchecked.

4. Click **Save Changes**.
5. Click **New Radius Rule** to add a new custom rule and provide the following information:
   - Name: A descriptive name
   - Response Packet Type: Access-Challenge
   - Reply-Message -- matches the expression: (.*)
   - Show GENERIC LOGIN page: Enable the check box

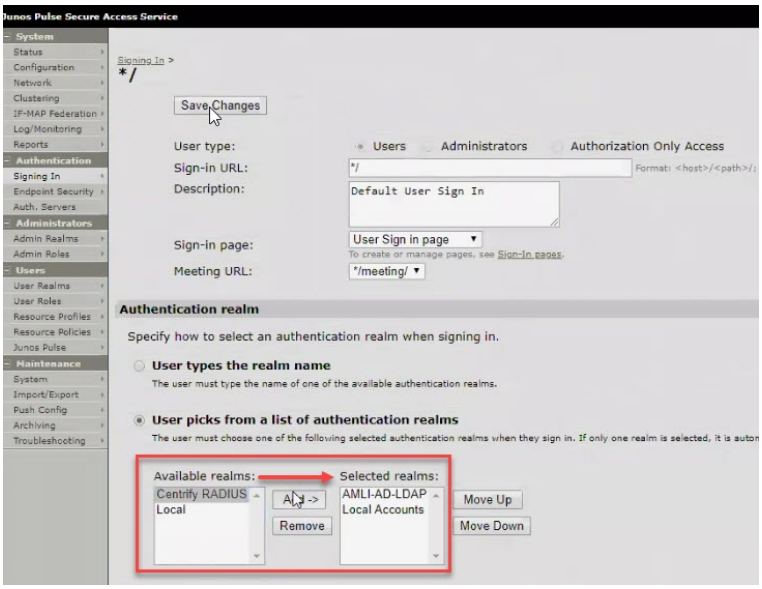
6. Click **Save Changes**.
7. Create another rule for the Access Reject packet type by clicking **Radius New Rule** and providing the following information:
   - Name: Enter a descriptive name
   - Response Packet Type: Access-Reject
   - Reply-Message - matches the expression: (.*)
   - Show GENERIC LOGIN page: Enable the check box
8. Click **Save Changes**.

   When you are done configuring the authentication rules, they should look similar to the following:
   - rule_1 - Access Challenge - (Reply-Message matches the expression "(.*)")
   - rule_2 - Access Reject - (Reply-Message matches the expression "(.*)")
9. Add the newly created Delinea RADIUS realm to the authentication realm.

a. Click **Authentication** > **Signing In** > the relevant User URL.



b. Move the newly created realm from the "Available realms" area to the "Selected realms" area.

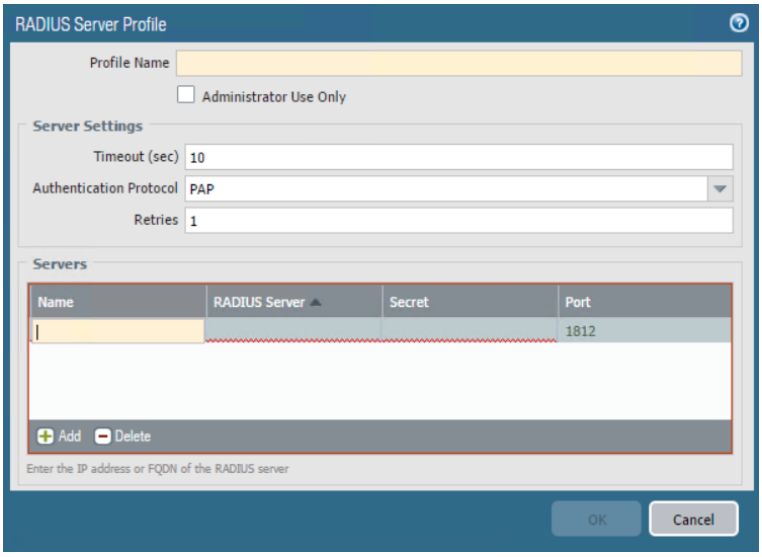


10. Click **Save Changes**.

To configure RADIUS authentication on a Palo Alto Networks device:

1. Add a server profile.
   a. Open the Palo Alto Networks administration interface.
   b. Navigate to **Device**, **Server Profiles**, **RADIUS**.
   c. Click **Add** and enter a name for the profile.
   d. Provide the following information for the Server settings:
      i. Timeout (Sec): 120
      ii. Authentication Protocol: PAP
      iii. Retries: 1

e. Navigate to **Servers** and click **Add** to add a RADIUS server profile.



f. Provide the following information:

i. Name: Enter a descriptive name to identify this RADIUS server, such as Delinea RADIUS.

ii. RADIUS Server: The hostname or IP address of the Delinea Connector.

iii. Secret: The Client Secret that you entered in the RADIUS client settings in the DelineaAdmin Portal.

iv. Port: 1812

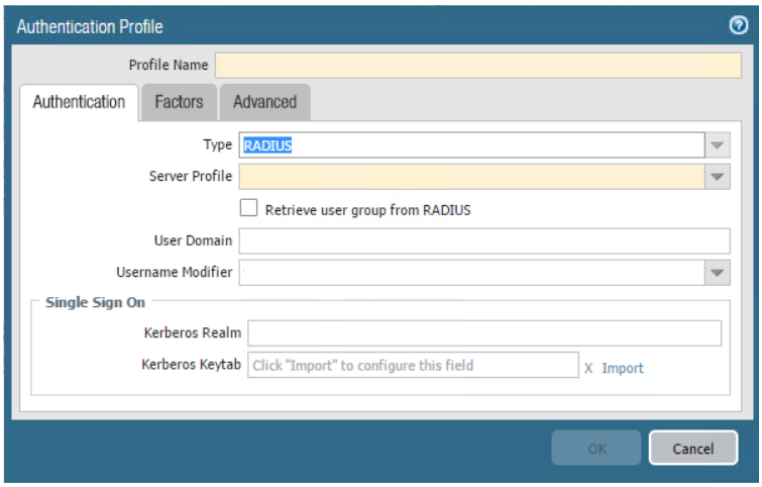
g. Click **OK** to save the profile.

2. Create an authentication profile.

a. Navigate to **Device**, **Authentication Profile,** click **Add** to enter a Name for the profile.

The authentication profile name cannot contain any spaces (for example, CentrifyAuth).

b. In the Authentication tab, select **RADIUS** from the Type drop-down menu.



c. Select the Server Profile you created for accessing your RADIUS server (for example, Delinea RADIUS).

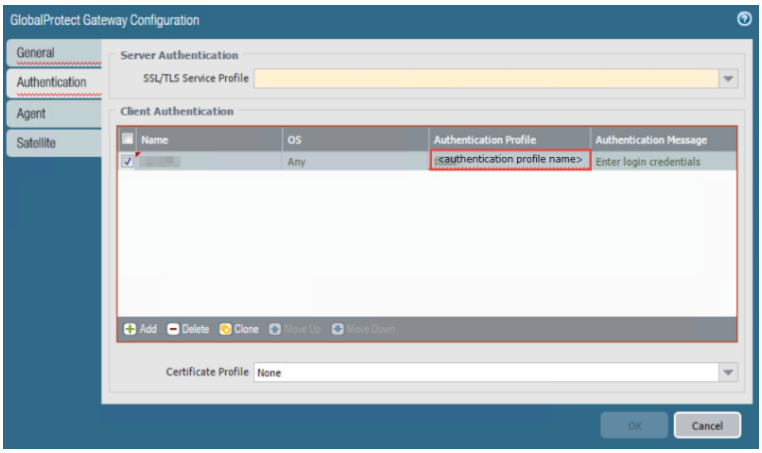
d. Click **OK** to save the authentication profile.

3. Configure the gateway(s).

a. Click the __Network__tab and select **GlobalProtect > Gateways** and select a configuration or Add one.

b. Click the **Authentication** tab, and then click **Add**.

c. Click the **Authentication Profile** field and from the drop down menu select the authentication profile you just created (for example, CentrifyAuth).



d. Enter an **Authentication Message** to let users know what authentication credentials to use.

e. Click **OK** to save the configuration.

4. Configure authentication override settings to accept secure, encrypted cookies.

a. Click **Network > GlobalProtect > Portals**, then open **GlobalProtect Portal Configuration**.

b. Click the **Agent** tab, then open **OnDemand-Profile**.

c. Click the **Authentication** tab, then select the following options:

i. **Generate cookie for authentication override**

ii. **Accept cookie for authentication override**

5. Set the global-protect timeout on the firewall device to 120 seconds.
   a. Connect to the firewall device via SSH.
   b. Enter the following commands:

```
\> configure
\# set deviceconfig setting global-protect timeout 120
\# commit
\# exit
```

Configuring the Delinea Connector for Use as a RADIUS Client

You can use your existing RADIUS server for user authentication into Privileged Access Service by enabling communication between your RADIUS server and the Delinea Connector (acting as a RADIUS client). The high level steps are:

1. Configure the RADIUS server to recognize the connector as a valid RADIUS client. See "Configuring a RADIUS Server" below.
2. Make configuration changes in Admin Portal to add RADIUS server information, designate the connector as a RADIUS client, and define your authentication requirements to include RADIUS. See "Configuring the Admin Portal (connector as a RADIUS client)" on the next page.

If you have multiple connectors enabled for use as RADIUS clients, Privileged Access Service prioritizes connection with the connectors in the following order:

1. Connectors from the same IP address as the user
2. Randomly chooses a connector if more than one is from the same IP address as the user
3. Choose the best subnet match
4. Randomly chooses a connector if none of the above are available

Configuring a RADIUS Server

You configure the RADIUS server to recognize the connector as a valid RADIUS client. The following RADIUS server configuration procedures use the RSA Authentication Manager's RADIUS interface as an example. Your procedure may differ slightly if you are using a different RADIUS server.

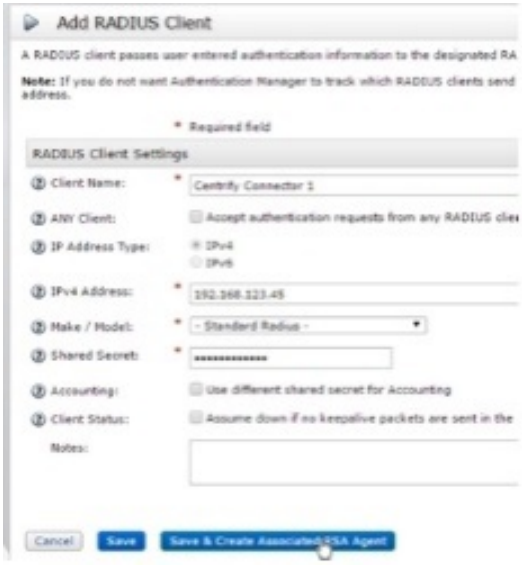
At a high level, you consistently need the following information regardless of the RADIUS server:

- IP address of the Delinea Connector
- The secret key you provide to the RADIUS server and Admin Portal must match exactly

To configure the RADIUS server (using the RSA Authentication Manager's RADIUS interface):

1. Log in to the Authentication Manager Security Console with "SuperAdmin" or "Auth Mgr Radius Admin" rights.
2. Click **RADIUS Clients > Add New** in the RADIUS area.

3. Provide the required information.



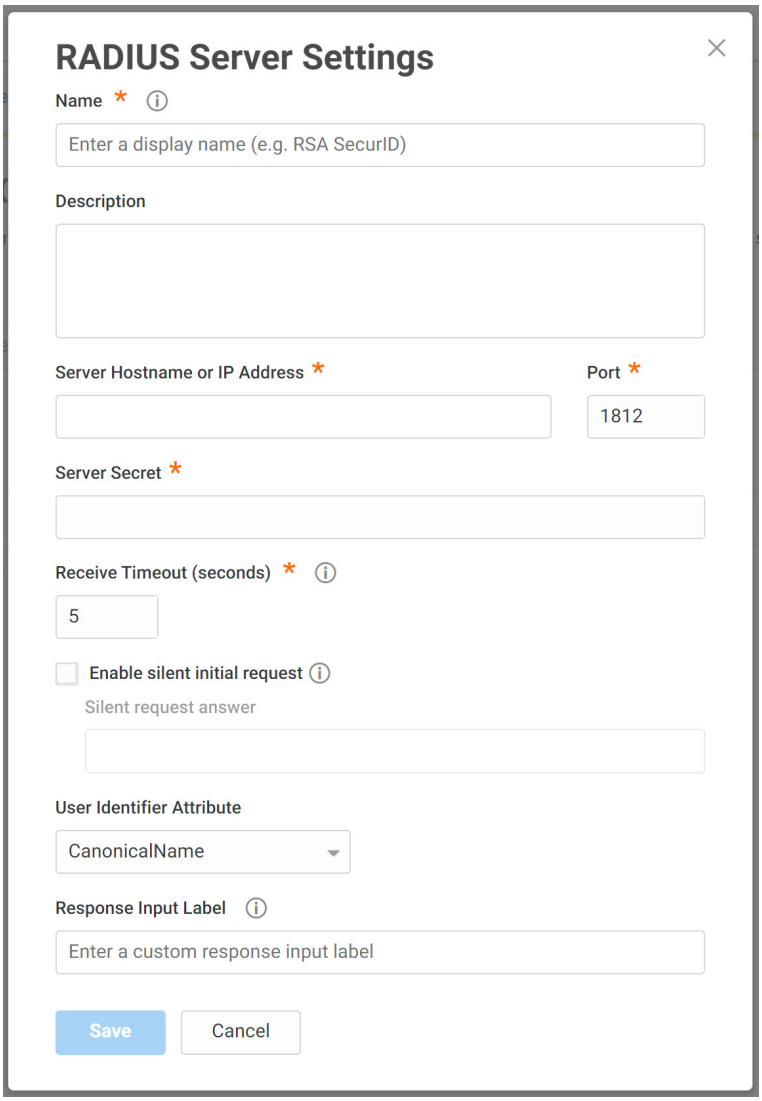
4. Click **Save and Create Associated RSA Agent**.

Configuring the Admin Portal (connector as a RADIUS client)

Make configuration changes in Admin Portal to add the RADIUS server information, designate the connector as a RADIUS client, and define your authentication requirements to include RADIUS.

To configure the connector and other Admin Portal settings:

1. Log in to Admin Portal.
2. Define the RADIUS server information:
   a. Click **Settings > Authentication > RADIUS Connections > Servers > Add** to define the RADIUS server information.



b. Define the relevant information:

Field	Entry
(Server) Name	The server name is displayed to users as one of their MFA mechanism options.
Server Hostname or IP Address + Port	The server hostname or IP address and port number.

Field	Entry
Server Secret	The Server Secret field is asking for the secret that is shared between the RSA server and Privileged Access Service. If you have entered a secret key on your RADIUS server, then enter that same key here. The keys must match to enable authentication. If you are creating a new secret key, best practices recommend 22 or more characters in length.
Receive Timeout (seconds)	Enter a value to specify the receive timeout for this server. The value must be no less than 5 seconds and no greater than 55 seconds.
Enable silent initial request + Silent request answer	Enable when this RADIUS server requires a fixed answer for the initial request. For example, using RSA Server with "Enable Only Additional Authentication" enabled. When this is chosen, the initial request to the server is sent with a username and whatever answer is specified in the **Silent request answer**.
(Optional) User Identifier Attribute	You can specify the attribute you want sent to the RADIUS client as the user name for authentication. You can select from the default list or define your own by selecting **Custom**. The `CanonicalName` default attribute is a computed value and is computed differently for each user type. For example, for Active Directory users it is set to one of the following (in this order): 1) `userPrincipalName` -- If the format is usable (not empty and does not start with "@"). 2) The concatenation of `sAMAccountName`, a "@", and the AD domain For Privileged Access Service users, it is computed as the contents of the `Name` field. The UUID default attribute represents the user ID stored in Privileged Access Service. When you define a Custom attribute, the named attribute must match exactly the user attribute name in the directory service. For example, you must use `sAMAccountName` instead of “sam account name” or “mail” instead of “Mail”.
Response Input Label	Set a custom label to use for the response input during login. Recommend 70 characters or less max.

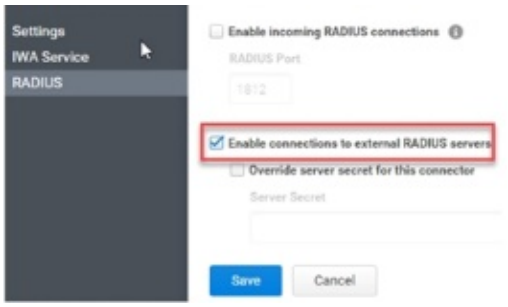
1. Click **Save**.
2. Configure the connector as a RADIUS client.

   All relevant connectors must be configured.

   a. Click **Network > Delinea Connector** > select an existing connector or add a new one to designate the connector as a RADIUS client.

      The Delinea Connector Configuration page opens.

   b. Click **RADIUS** and select the **Enable connections to external RADIUS server** check box.



c. (Optional) Select **Override server secret for this connector** check box.

d. If you do not want all your connectors to have the same shared secret, you can override the secret here and enter a different secret.

e. Click **Save**.

3. Enable 3rd party RADIUS authentication.

a. Click **Policies** and either select an existing policy set or add a new one.

b. Click **User Security Policies > RADIUS**.

c. Select **Yes** in the Allow 3rd Party RADIUS Authentication dropdown.

This setting allows users to authenticate using the RADIUS server.

d. Click **Save**.

4. Define your authentication requirements to specify when and under which conditions your users will authenticate using the RADIUS server. See "How to Define Authentication Requirements" on page 280. The authentication profile you choose must have the “3rd Party RADIUS Authentication” mechanismselected. Users will not be able to authenticate using the RADIUS server until you define the authentication requirements.

Users can now log in to Privileged Access Service by selecting the RADIUS server authentication method and entering the passcode generated by the RADIUS token container application -- which mirrors a hardware token or a token container running on a mobile device.

How to Configure OAuth 2.0 Flows

OAuth 2.0 is an open-standard framework and specification for authorizing client applications to access online resources. Authorization works by requiring a client to obtain an access token from a server that in turn grants the client access to specific protected resources. The client then sends the access token to the resource whenever it invokes the resource's endpoints.

Privileged Access Service support OAuth 2.0, allowing custom Delinea client applications access to online resources needed by those applications.

Refer to https://developer.centrify.com/docs/oauth for more information about using OAuth 2.0. with Delinea.

Flows that Privileged Access Service support are:

Flow	Description
Client Credentials	The client application must provide a client ID and client secret to obtain an access token from a tenant.
Authorization Code	The client redirects the user to the OAuth authorization endpoint where the user enters their credentials and grants access. The OAuth server then returns an authorization code to the client. The client then sends a request to the OAuth token endpoint to obtain an access token, and includes the authorization code in this request. The OAuth server then returns the authorization (and refresh token if it's configured) to the client for use in accessing subsequent endpoints.
Implicit	The client redirects the user to the OAuth authorization endpoint where the user enters their credentials and grants access. The OAuth authorization endpoint then redirects the user back to the client application and includes the access token in the redirection. The client can then use the access token for use in accessing subsequent endpoints. This flow is the simplest and is typically used by Javascript applications running in a browser. Since the access token under this flow is assumed to be used temporarily, no refresh token is issued by the OAuth server.
Resource Owner	The client application provides its own user interface in which the user enters their credentials and grants access to resources. This information is then sent to the OAuth token endpoint which returns an access token to the client. Since this flow does not involve redirection to an OAuth authorization endpoint to obtain authorization, it should only be used in highly privileged client applications such as native applications running on an OS.

Refer to https://developer.centrify.com/docs/oauth for more information about using OAuth 2.0.with Delinea.

Refer to the following topics for an overview of the OAuth2 client and server applications used to configure access to your Delinea tenant:

- "Custom Oauth2 Client" below

  Use the custom OAuth2 Client application if the resulting access token is used to call Privileged Access Service APIs.

- "Custom Oauth2 Server" on page 344

  Use the custom OAuth2 Server application for use with another web application's APIs. With the OAuth2 Server application, you can set custom claims in the resulting access token.

Custom OAuth2 Client

Custom Oauth2 Client

OAuth 2.0 is an open-standard framework and specification for authorizing client applications to access online resources. Authorization works by requiring a client to obtain an access token from a server that in turn grants the

client access to specific protected resources. The client then sends the access token to the resource whenever it invokes the resource's endpoints.

Privileged Access Service support OAuth 2.0, allowing custom Delinea client applications access to online resources needed by those applications.

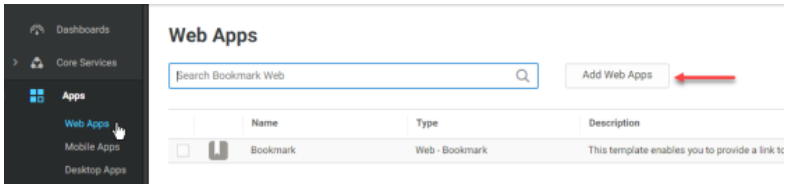
This topic covers how to add the custom OAuth2 Client application to the Admin Portal and describes the available configuration fields and options.

Use the custom OAuth2 Client application if the resulting access token is used to call Privileged Access Service APIs.

Refer to https://developer.centrify.com/docs/oauth for more information about using OAuth 2.0.with Delinea.

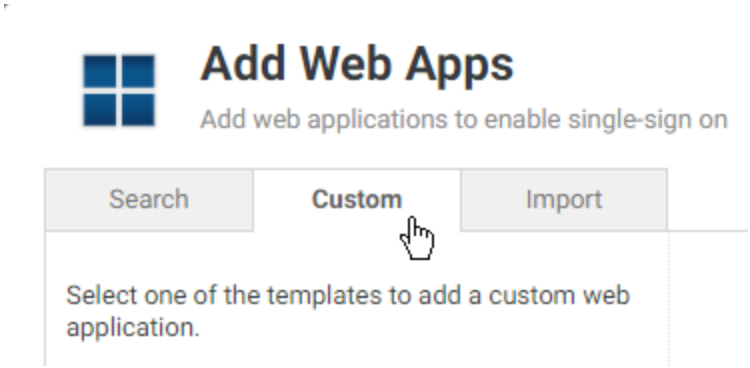
To add and configure a custom OAuth 2.0 client:

1. In the Admin Portal, select **Apps > Web Apps**, then click **Add Web Apps**.



   The Add Web Apps screen appears.

2. Click **Custom**.

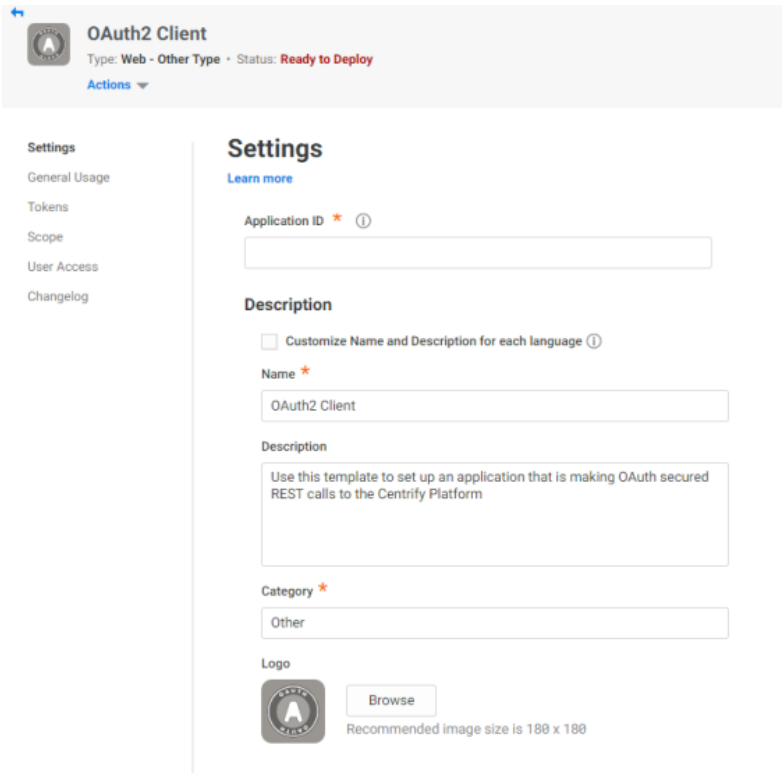


3. On the Custom tab, next to the **OAuth2 Client** application, click **Add**.
4. In the Add Web App screen, click **Yes** to add the application.

   The Admin Portal adds the application.

5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Settings page.

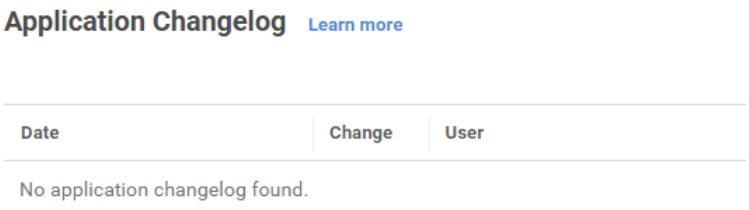


6. On the Settings page, complete the following fields:
   - **Application ID**: a unique key used to build the OAuth2 endpoint URL (URL format is tenant.my.centrify.net/oauth2/introspect/appID.
   - **Customize Name and Description for each language**: allows you to specify a name and description for this app, per supported language.
   - **Application Name**: a descriptive name for the application.
   - **Application Description**: a description for the application.
   - **Logo**: you can optionally provide a logo to identify your app.
7. On the **General Usage** page, complete the following fields to specify the types of credentials that can be used to authorize with this server:
   - **Client ID Type:** choose one of these options:
     - **Anything:** allows for authorization in any client where authorization is granted by the user (for example, in a popup screen).
     - **List:** - specifies a list of clients who are allowed access. Click **Add** and then enter the application name of your client.
     - **Confidential:** requires an OAuth2 client to send a client ID and secret. A confidential client is recommended for all flows, but is only required for the Client Credentials flow.
   - **Issuer:** the URL of the server issuing access tokens. Can be left as default.

- **Allowed Redirects:** specifies the redirects that should be trusted when redirection occurs during the *Authorization Code* and *Implicit*flows. Not applicable for the *Client Credential* and *Resource Owner* flows.

8. On the **Tokens** page, complete the following fields:
   - **Token Type:** specifies the type of token to issue (JwtRS256 or opaque). JwtRS256 is a JSON Web Token (JWT) composed of Base64 encoded user and claim information. An opaque token contains no information about the user. To obtain user and claim information for an opaque token an introspection URL must be used by passing the token. The format of the introspection URL is tenant.my.centrify.net/oauth2/introspect/appID.
   - **Auth Methods:** specifies the authentication flow(s) for which the specified token type should be issued.
   - **Token Lifespan:** specifies the token's lifespan.
   - **Issue refresh tokens:** when enabled, allows clients to request a refresh token that can be exchanged for a new access token. Not applicable for the Resource Owner or Client Credentials flows.
9. On the **Scope** page, add any desired scopes and select from the following options:

   Refer to https://developer.centrify.com/docs/client-credentials-flow#section-step-3-create-scopes for more information about creating scopes.
   - **User must confirm authorization request**: Select this option if you want to the user to confirm the authorization request before receiving a token.
   - **Allow scope selection**: Select this to give users the option of choosing from the scopes that you added.
10. On the **User Access** page, select the role(s) that the user must be in, in order to authorize against the server.
11. (Optional) On the **Changelog** page, you can see recent changes that have been made to the application settings, by date, user, and the type of change that was made.



12. Click **Save**.

Custom OAuth2 Server

Custom Oauth2 Server

OAuth 2.0 is an open-standard framework and specification for authorizing client applications to access online resources. Authorization works by requiring a client to obtain an access token from a server that in turn grants the client access to specific protected resources. The client then sends the access token to the resource whenever it invokes the resource's endpoints.

Privileged Access Service support OAuth 2.0, allowing custom Delinea client applications access to online resources needed by those applications.

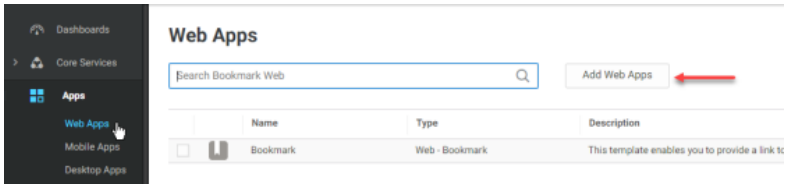
This topic covers how to add the custom OAuth2 Server application to the Admin Portal and describes the available configuration fields and options.

Use the custom OAuth2 Server application for use with another web application's APIs. With the OAuth2 Server application, you can set custom claims in the resulting access token.

Refer to https://developer.centrify.com/docs/oauth for more information about using OAuth 2.0. with Delinea.

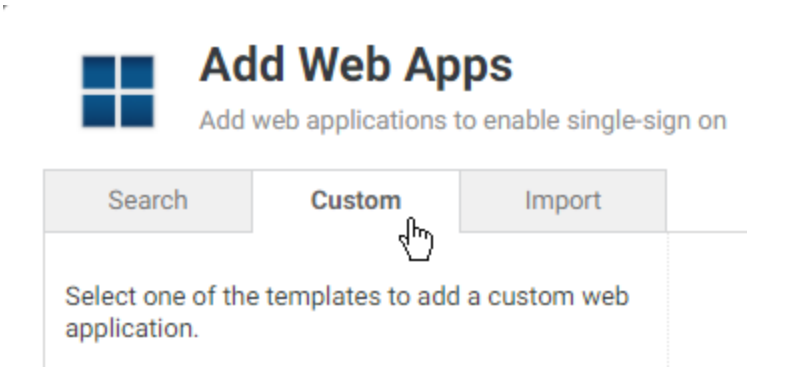
To add and configure a custom OAuth 2.0 Server application:

1. In the Admin Portal, select **Apps > Web Apps**, then click **Add Web Apps**.



   The Add Web Apps screen appears.

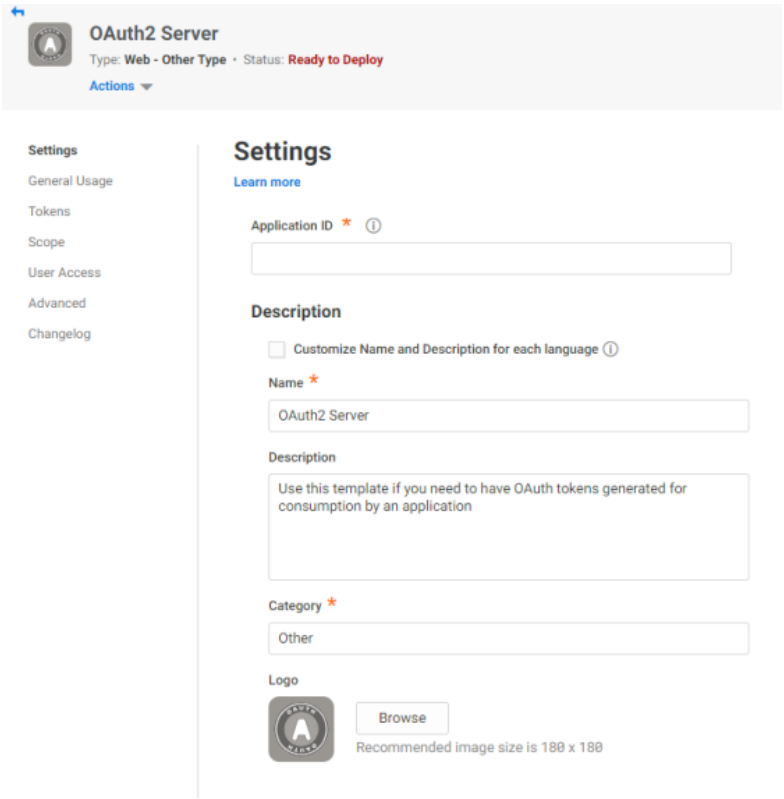
2. Click **Custom**.



3. On the Custom tab, next to the **OAuth2 Server** application, click **Add**.
4. In the Add Web App screen, click **Yes** to add the application.

   The Admin Portal adds the application.
5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Settings page.

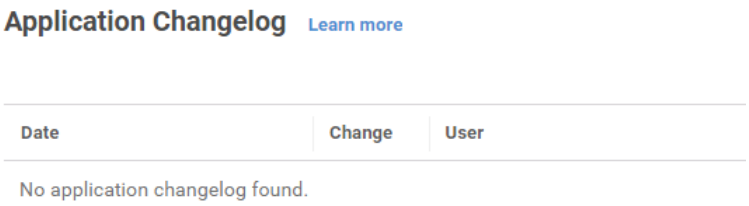


6. On the Settings page, complete the following fields:
   - **Application ID**: a unique key used to build the OAuth2 endpoint URL (URL format is tenant.my.centrify.net/oauth2/introspect/appID.

- **Customize Name and Description for each language**: allows you to specify a name and description for this app, per supported language.
- **Application Name**: a descriptive name for the application.
- **Application Description**: a description for the application.
- **Logo**: you can optionally provide a logo to identify your app.

7. On the **General Usage** page, complete the following fields to specify the types of credentials that can be used to authorize with this server:
   - **Client ID Type:** choose one of these options:
     - **Anything:** allows for authorization in any client where authorization is granted by the user (for example, in a popup screen).
     - **List:** - specifies a list of clients who are allowed access. Click **Add** and then enter the application name of your client.
     - **Confidential:** requires an OAuth2 client to send a client ID and secret. A confidential client is recommended for all flows, but is only required for the Client Credentials flow.
   - **Issuer:** the URL of the server issuing access tokens. Can be left as default.
   - **Audience:** metadata that a client may use to verify that the tokens it receives are correct (i.e., allows for client-side verification of a token). Can be set to any string. For example, a client may use this field to ensure a match on the issuer.
   - **Allowed Redirects:** specifies the redirects that should be trusted when redirection occurs during the *Authorization Code* and *Implicit*flows. Not applicable for the *Client Credential* and *Resource Owner* flows.
8. On the **Tokens** page, complete the following fields:
   - **Token Type:** specifies the type of token to issue (JwtRS256 or opaque).

     JwtRS256 is a JSON Web Token (JWT) composed of Base64 encoded user and claim information. An opaque token contains no information about the user. To obtain user and claim information for an opaque token an introspection URL must be used by passing the token. The format of the introspection URL is tenant.my.centrify.net/oauth2/introspect/appID .
   - **Auth Methods:** specifies the authentication flow(s) for which the specified token type should be issued.
   - **Token Lifespan:** specifies the token's lifespan.
   - **Issue refresh tokens:** when enabled, allows clients to request a refresh token that can be exchanged for a new access token. Not applicable for the Resource Owner or Client Credentials flows.
9. On the **User Access** page, select the role(s) that the user must be in, in order to authorize against the server.
10. (Optional) On the **Advanced** page, you can enter a custom script that sets claims for JWTs being issued by the tenant for the server.
11. (Optional) On the **Changelog** page, you can see recent changes that have been made to the application settings, by date, user, and the type of change that was made.



12. Click **Save**.

How to Configure OATH OTP

You can enable users to scan a Delinea generated QR code (using a third party authenticator application or the Delinea application) to authenticate to Privileged Access Service. A one-time-passcode (OTP) is displayed and users can use that OTP to log in to Privileged Access Service. You can direct users to "Using OTPs to Authenticate" on page 364.

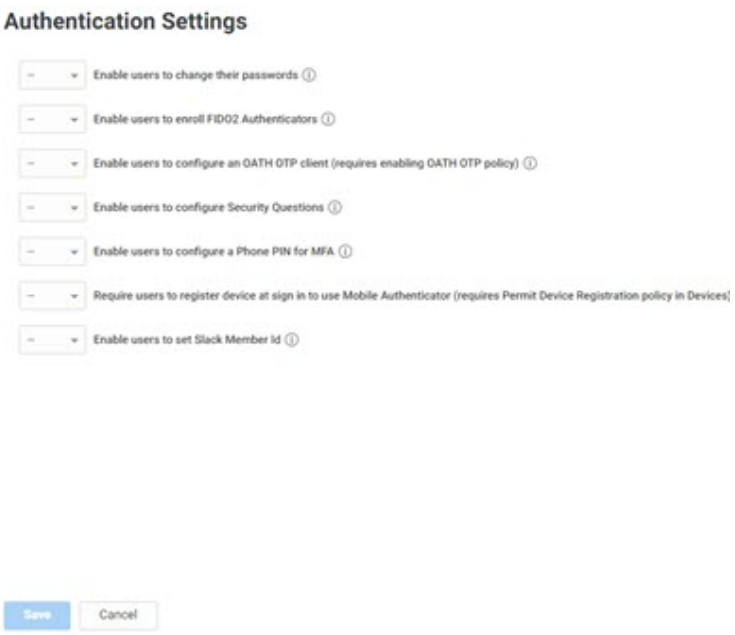
Additionally, you can upload existing OATH tokens and allow users to authenticate using the one-time passcode generated from those tokens. See "Importing OATH Tokens in Bulk" on the next page

Important: You must configure an authentication rule with the OATH OTP mechanism enabled in the associated authentication profile for the relevant policy. If you do not have this configured, users will not be able to authenticate using the QR code. See "Creating Authentication Rules" on page 281.

To Enable the OTP Policy

1. Log in to Admin Portal
2. Click **Access > Policies**.
3. Select a policy set or create a new one.
4. Click **User Security > OATH OTP**.
5. Select **Yes** in the **Allow OATH OTP Integration** drop down.
6. Click **Save**.
7. Select the policy you created. Enable users to configure an OATH OTP client.
   a. Select **User Security > Authentication Settings**.

      The Authentication Settings window opens.



b. Select **Yes** in the **Enable user to configure an OATH OTP client**.

c. Enter a user-friendly name (for example the name of the OTP client used by your organization) in the **OATH OTP Display Name** text field. This name is what users will see.

d. Select an authentication profile to require users to provide additional authentication before they can access the QR code.

8. Click **Save**.

Importing OATH Tokens in Bulk

You can authenticate with Privileged Access Service using your existing third-party OATH tokens (for example, those generated by a YubiKey) by bulk uploading those tokens. Privileged Access Service uses those tokens to generate one-time passcodes (OTP) that users with registered devices can immediately use to log in to the admin portal.

Users without registered devices must first log in to the Admin Portal and scan the Privileged Access Service generated QR code (using a third party authenticator) to get the passcode pushed to their devices. You can direct users to "Using OTPs to Authenticate" on page 364.

When you upload these tokens, they will override any existing passcode users may have generated by scanning the Privileged Access Service generated QR code.

Prepare the CSV File

Prior to importing OATH tokens, you need a CSV file containing information for each token. Privileged Access Service validates one OATH token per user. If your CSV file contains more than one OATH token for the same user, the last token (the one lowest in the spreadsheet) is validated for that user.

The CSV file must contain the following column headers and the header names must match the ones listed below:

Note: A CSV file template is available on the bulk upload page in Admin Portal.

- **User Principle Name:** Required. Username associated with the user's account. This is typically the user's email address.
- **Token Identifier:** Optional. A unique identifier used to associate multiple OATH OTP tokens with the same user.
- **Secret Key (HEX):** Required. An arbitrary key value in HEX format.
- **Account Name:** Required. The name for the user's account.
- **Issuer:** Optional, but strongly recommended. A string value specifying the associated provider or service for this account.

  Note: The string must be URL-encoded according to RFC 3986

  If the issuer parameter is not provided, the issuer information may be pulled from the label's issuer prefix.

  For example, the valid value to the following label prefix example would be

  ```
  issuer=Example:
  otpauth://totp/Example:alice@google.com?secret=JBSWY3DPEHPK3PXP&issuer=Exampl
  ```

  Note: Older Google Authenticator implementations ignore the issuer parameter and rely on the issuer label prefix to disambiguate accounts. Newer implementations will use the issuer parameter for internal disambiguation, and the parameter will not be displayed to the user. We recommend you use both the issuer label prefix and the issuer parameter to safely support both the old and new Google Authenticator versions.

- **Algorithm:** Optional. Algorithm used to process the information. Algorithm may have one of the following values:
  - `SHA1` (Default)
  - `SHA256`
  - `SHA512`

  Note: Currently, the algorithm parameter is ignored by Google Authenticator implementations.

- **OTP Digits:** Optional. Determines the display time of the one-time passcode shown to the user. OTP digits may have the values 6 (default) or 8.

  Note: Currently, for Android and Blackberry devices, the digits parameter is ignored by Google Authenticator.

- **Type:** Required. Determines if the key will be used for counter-based HOTP or for TOTP. Valid type values are `hotp` and `totp`.
- **Period:** Optional when the type value is `totp`. Defines the time (in seconds) that a TOTP code is valid. The default value is 30.

  Note: Currently, the period parameter is ignored by Google Authenticator implementations.

- **Counter:** Required when the type value is `hotp`. Sets the initial counter value.

Upload OATH Tokens

To bulk upload OATH tokens:

1. Log in to Admin Portal.
2. Navigate to **Access > OATH Tokens**.
3. Click **Bulk Token Import**.
4. Click **Browse**, navigate to your CSV file, and upload it.
5. Click **Next**.
6. Review the first 15 rows and if they look correct, click **Next**.

   If you see an error, cancel the upload and fix the error.
7. Confirm the email address or enter a different one where a bulk import report will be sent.
8. Click **Confirm**.

   A bulk import report email is sent to the specified email address.
9. Refresh the OATH Tokens page to see the uploaded instance.

   If you have not configured the OATH OTP policy, you need to do so before users can use the generated passcodes. When you configure the OATH OTP policy, you can also define if users can see the QR code from the Admin Portal. See "How to Configure OATH OTP" on page 347.

How to Configure MFA for Third-Party Integration

Using the Delinea PAS, you can configure multi-factor authentication (MFA) for VPN connections. The configuration requires calling an API to invoke a specific MFA policy defined in **Access** > **Policies** > **Third Party Integration**.

See On Demand Challenge API for details on the API.

For information about using a RADIUS server here, you can configure the connector to act as a RADIUS server. For details, see "Configuring the Delinea Connector for Use as a RADIUS Server" on page 324.

How to Use MFA Redirection

Multi-Factor Authentication (MFA) redirection enables users to perform MFA on behalf of any chosen user. This means the user that is logging in can be configured to perform MFA as the redirect user, and receive an identity token for the original login user after they successfully login.

Once configured, the MFA redirection is handled automatically.

Note: When you log in to an enrolled system and your account is set up to use MFA redirection, the service prompts you for your password, not the password for the MFA redirect user. This feature is available on systems that have the Centrify Client installed and enrolled

How MFA Redirection Works

To explain how redirection works, we've defined the following two users:

- **Original login user:** The user who is actively trying to log in.
- **Redirect user:** The user who has MFA setup. MFA will redirect to this user to answer any MFA challenges.

MFA is performed as the redirect user, on behalf of the original login user. This means any MFA mechanism that is used (i.e. email, text, Mobile Authenticator, etc.) all are completed by the redirect user.

Note: When MFA redirect is setup, cloud clients are provided with the redirect user's information and MFA challenges. This means the original login user enters the system as the redirect user.

The general MFA redirection flow is:

1. The original user attempts to login with their username.
2. The details for the original login user are retrieved from Delinea PAS.
3. The original login user receives MFA challenges for the redirect user's account.
4. When authentication is successful, the account details for the redirect user's account are shown to the original login user, and an identity token/cookie is provided to the original login user.

In a typical use case:

- The original login user has no attributes configured, and therefore they cannot satisfy any MFA.

  When the original login user is challenged for additional authentication, the MFA redirection feature can be configured so the redirect user's MFA challenges (who has the required mechanisms configured) are used for the original login user to answer.
- The redirect user will have all their account challenge attributes set:
  - Phone number
  - Configured security questions
  - Yubikey
  - Mobile Authenticator
  - etc.

This enables the original login user to satisfy the MFA requirement through answering the redirect user's MFA challenge(s).

The MFA redirect process acts as if the redirect user was directly logging in. The redirect user just facilitates the act of MFA, which causes any actions available during the login process (password reset, forgot password, account unlock, etc.) to apply to the redirect user's account, even though the original login user is the one using the login.

However, once the login is complete, the login identity will be granted to the original login user, and any actions (password reset, forgot password, account unlock, etc.) will apply back to the original login user's account.

MFA Examples

Phone MFA example:

- The original login user configures their account to have MFA redirected through the redirect user.
- The MFA is set up to use a phone number for authentication.

Since the original login user is configured for MFA redirection, the original login user can request the redirect user's phone number MFA challenge, in order to satisfy the phone MFA challenge required to login.

The policy and authentication rules for the original login user still apply whether redirection is used or not. The specified MFA redirect user will be used to determine which MFA mechanisms are able to be satisfied, as well as perform MFA.

Real-world example:

A real-world use case is when an admin (the original login user) uses their dash-A account to perform a privileged task rather than their normal enterprise account (the redirect user). The admin does not have a phone enrolled with their dash-A account but they do with their normal enterprise account. They do have the Mobile Authenticator associated with their enterprise account. MFA redirection enables the admin to carry one phone rather than two and use the Mobile Authenticator to satisfy the MFA.

How to Set Up MFA Redirection

Note: You must have the MFA Redirect Management permission in order to set redirect for a user. All system admins already have this right applied to their account.

To configure a user for MFA redirection:

1. From the Admin Portal, navigate to **Access** > **Users**.
2. Click on the user account you want to configure for MFA redirection.
3. Ensure you're on the **MFA Redirection** tab and check the **Redirect Multi-factor Authentication to a different user account** box.
4. On the user selector, click **Select**.
5. Search for the user you want to use for the MFA redirection. Select the user you want to use and click **OK**.

   Note: If you select a user that is the same as the user you're currently editing, you will generate an error.

6. Click **Save**.

Preparing Authentication Profiles

With Privileged Access Service, you can require multi-factor authentication for two distinct situations:

- As part of the **login** process so that users who are attempting to log in to Delinea-managed computers must provide multiple forms of authentication before they are granted access.
- As part of a **re-authentication** process so that users who are attempting to use Application, Network, and Desktop rights on Windows machines, orcommand rights with elevated privileges or in a restricted shell on UNIXmachines, must provide a password and another form of authentication before they can execute the selected command.

To configure the types of authentication challenges allowed in each situation, you can prepare one or more **authentication profiles** in the Admin Portal. If you have already configured authentication profiles for other purposes, you can reuse those profiles for multi-factor authentication or add new profiles specifically for the computers you manage using Delinea Server Suite. You can prepare one profile to use for both login access and for the use elevated privileges or you can prepare separate profiles for each situation.

To create an authentication profile:

The first step in preparing authentication profiles is to create the profile.

1. Open a browser and log on to the Privileged Access Service using your customer-specific URL.
2. Switch to the administrative portal, then click **Settings** and click **Authentication**.

   Three default authentication profiles are available out-of-the-box:

   - Default New Device Login Profile: Uses Password for the first challenge and Mobile Authenticator, Text message (SMS) confirmation code, Emailconfirmation code, or OATH OTP Client for the second challenge with a 12 hours pass-through duration.
   - Default Other Login Profile: Uses Password for the first challenge and no secondary challenge with a 12 hours pass-through duration.
   - Default Password Reset Profile: Gives the option for users to use Mobile Authenticator, Text message (SMS) confirmation code, Email confirmationcode, or OATH OTP Client for the first challenge with a 12 hours pass-through duration.
3. Select an existing Authentication Profile or click **Add Profile**.

   The fields needed to **add new profile**.

   a. Type the authentication profile name.

   b. Select the types of authentication to present for the first challenge.

      Note: The second authentication is not needed. Challenge two is a third mechanism.

   c. Click **OK**.

      The pass-through option applies to Active Directory user MFA logins on systems that are joined to Active Directory.

      Note: Only the authentication challenges that are applicable for a user can be presented. For example, you might select Phone call and Email confirmation code in the authentication profile, but these challenges are only valid if users have both a phone number and email address stored for their accounts. If users only have a phone number and not an email address stored, they will receive a phone call to complete the authentication process rather than be prompted to select an authentication option. If users have both a phone number and an email address stored, they will be prompted to select which form of authentication to use.

   - Select the authentication mechanism(s) you require and want to make available to users. Some authentication mechanisms require additional configurations before users can authenticate using those mechanisms. See Authentication mechanisms for information about each authentication mechanism. For example, you can require that the first challenge be the user's account password. Then for the second challenge, users can choose between an email confirmation code, security question, or text message confirmation code.
   - If you have multiple challenges, Privileged Access Service waits until users enter all challenges before giving the authentication response(pass or fail). For example, if users enter the wrong password for the first challenge, we will not send the authentication failure message until after users respond to the second challenge.

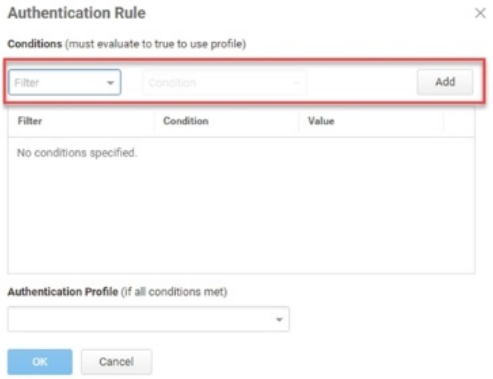
- If users fail their first challenge and the second challenge is SMS, email, or phone call, the default configuration is that Privileged Access Service will not send the SMS/email or trigger the phone call. Contact support to change this configuration.

Assigning Login Authentication Profiles

The next step is to assign login authentication profiles. Do this by performing the following steps.

1. Click **Access > Policies** and **Add Policy Set**. Under **Policy Settings**, navigate to **Login Policies**. Choose between Linux, UNIX and Windows Servers and Windows Workstations.
2. Select **Yes** in the **Enable authentication policy controls** drop-down.Click **Add Rule**.

   The Authentication Rule window displays.
3. Click **Add Rule** on the Authentication Rule window.
4. Define the filter and condition using the drop-down boxes.



For example, you can create a rule that requires a specific authentication method when users access Privileged Access Service from an IP address that is outside of your corporate IP range. Supported filters are:

Filter	Description
IP Address	The authentication factor is the computer's IP address when the user logs in. This option requires that you have configured the IP address range in Settings, Network, Corporate IP Range.
Day of Week	The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.
Date	The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.
Date Range	The authentication factor is a specific date range.

Filter	Description
Time Range	The authentication factor is a specific time range in hours and minutes.
Device OS	The authentication factor is the device operating system.
Country	The authentication factor is the country based on the IP address of the user computer.
Risk Level	Risk Level: The authentication factor is the risk level of the user logging on to Admin Portal. For example, a user attempting to log in to Privileged Access Service from an unfamiliar location can be prompted to enter a password and text message (SMS) confirmation code because the external firewall condition correlates with a medium risk level. This Risk Level filter, requires additional licenses. If you do not see this filter, contact Delinea support. The supported risk level are: Non Detected -- No abnormal activities are detected. Low -- Some aspects of the requested identity activity are abnormal. Remediation action or simple warning notification can be raised depending on the policy setup. Medium -- Many aspects of the requested identity activity are abnormal. Remediation action or simple warning notification can be raised depending on the policy setup. High -- Strong indicators that the requested identity activity is anomaly and the user's identity has been compromised. Immediate remediation action, such as MFA, should be enforced. Unknown -- Not enough user behavior activities (frequency of system use by the user and length of time user has been in the system) have been collected.
Managed Devices	The authentication factor is the designation of the device as “managed” or not. A mobile device is considered “managed” if it is managed by Privileged Access Service (MDM enrolled), or if it has a Privileged Access Service-trusted certificate authority (CA has been uploaded to your tenant using Admin Portal > Settings > Authentication > Certificate Authorities).

5. Click the **Add** button associated with the filter and condition.
6. Select the profile you want applied if all filters/conditions are met in the **Authentication Profile** drop-down.
7. The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the**Add New Profile** option.
8. Click **OK**.
9. Select a default profile to be applied if a user does not match any of the configured conditions in the **Default Profile (used if no conditions matched)** drop-down.

   Note: If you have no authentication rules configured and you select **Not Allowed** in the **Default Profile** dropdown, users will not be able to log in to the service.

10. Click **Save**.
11. If you have more than one authentication rule, you can prioritize them on the **Login Authentication** page.

Assigning Privilege Elevation (Re-authentication) Profile

Finally, you must assign privilege elevation profiles.

1. For Elevated Privileges Profile, click **Privilege Elevation Policies > Privilege Elevation**, select **Yes** for Enable authentication policy controls, and **Add Rule > Add Filter**, click **Authentication Profiles**and display the list of existing profiles and select a profile to use or click **Add New Profile**.

   You can use the same profile for server access, and to re-authenticate for roles and rights that require multi-factor authentication. However, if you want to specify different authentication challenges from which a user can select when executing UNIX commands or accessing Windows applications, select **Add New Profile**.

   As with the Login Authentication Profile, you can select multiple types of authentication to present for the first and second challenges. However, only the authentication challenges that are applicable for a user can be presented when the user attempts to access privileged Windows rights or execute UNIX commands with elevated privileges (`dzdo`) or in a restricted shell (`dzsh`).
2. Click **Save**.

Reference Content – Authentication

You can specify what authentication mechanisms your users need to provide to access the service, as well as if and when multifactor authentication is required. For example, you can create a rule to require that users provide a password and text message confirmation code if they are coming from an IP address that is outside of your corporate IP range. To specify this requirement, you need to create a rule and associate it with an authentication profile.

This section contains the following topics:

Authentication Mechanisms

You can select the authentication mechanisms that will be available to users. However, the mechanisms ultimately offered to users on the login prompt depend on the account's properties. For example, if you select all of the mechanisms but a user account has only a user name and email address, then the login prompt will only offer those two options.

To set the authentication mechanisms, see "Creating Authentication Profiles" on page 284.

The following mechanisms are available:

- **Password**

  When you select this option, users are prompted for either their Active Directory or Privileged Access Service user password when logging in to the Admin portal.
- **Mobile Authenticator**

  When you select this option, users authenticate using a one-time passcode displayed by the Delinea application installed on their mobile devices.

If devices are connected via the cell network or a wi-fi connection, users can send the passcodes from the devices. If the devices are not connected, users must manually enter the passcodes into the Admin Portal login prompt.

This option requires users to have Delinea application installed on their devices and those devices must be registered in Privileged Access Service.

- **Phone call**

  When you select this option, Privileged Access Service calls the user using the stored phone number (mobile or land line) and describes an action theuser must perform to complete the authentication. The user completes theaction from the device to log in. If your tenant is configured on PrivilegedAccess Service 17.10 or newer, see "Enabling Phone PIN" on page 287 because additional configuration is required.

  This option is disabled for new tenants by default. Contact Delinea Support to enable this authentication mechanism.

- **Text message (SMS) confirmation code**

  When you select this option, Privileged Access Service sends a text message to the user's mobile phone with a one-time confirmation code and/or anauthentication link. Depending on the language setting, some languagesdisplay only the confirmation code while others display the confirmationcode and link. Users who are connected to the Internet can click/tap thelink. Otherwise, they need to enter the confirmation code in the login prompt.

  You can configure the confirmation code length (6 or 8 digits) in **Admin Portal** > **Settings** > **Authentication** > **Security Settings** > **Email and SMS passcode length** drop down option. The default is 8 digits.

  Note: The link and confirmation code are valid for 20 minutes. If a user does not respond within this time period, the Privileged Access Service cancels the login attempt.

  This option is disabled for new tenants by default. Contact Delinea Support to enable this authentication mechanism.

- **Email confirmation code**

  When you select this option, Privileged Access Service sends a confirmation code and a link to the user's email address. Users who are connected to the Internet can click/tap the link. Otherwise, they need to enter the confirmation code in the login prompt.

  You can configure the confirmation code length (6 or 8 digits) in **Admin Portal** > **Settings** > **Authentication** > **Security Settings** > **Email and SMS passcode length** drop down option. The default is 8 digits.

  The link and confirmation code are valid for 20 minutes. If a user does not respond within this time period, the Privileged Access Service cancels the login attempt.

- **FIDO2 Authenticator(s)**

  FIDO2 is an authentication standard hosted by FIDO Alliance. This standard includes the Web Authentication ("WebAuthn") API, which is a specification written by the World Wide Web Consortium (W3C) and FIDO, with participation from additional third parties. The WebAuthn API is backward compatible with Universal 2nd Factor (U2F) keys.

  Delinea leverages the WebAuthn API to enable password less authentication to the Privileged Access Service using either on-device or external authenticators. On-device authenticators are biometric authenticators

integrated into the device hardware. Popular examples are Mac Touch ID, Windows Hello, and fingerprint scanners. External authenticators are security keys that you plug into the device's USB port; for example, a YubiKey.

- **Security Question(s)**

  When you select this option, users are prompted to answer user-defined and/or admin-defined security questions. When creating the authentication profile, you can specify the number of questions users must answer. You can also specify the number of user-defined and admin-defined questions available to users. See "Enabling Multiple Security Questions" on page 288.Users create, select, or change the question and answer from their Account page in the Admin Portal.

- **OATH OTP Client**

  This text string is configurable and reflects what you entered during the OATH OTP configuration. When you select this option, users can use a third party authenticator (like Google Authenticator) to scan a Privileged Access Service generated QR code and get a one-time-passcode (OTP). This authentication mechanism requires additional configurations. "How to Configure OATH OTP" on page 347.

- **3rd Party RADIUS Authentication**

  When you select this option, we communicate with your RADIUS server to allow for user authentication into Privileged Access Service.

What You Need for Each Authentication Mechanism

The following table lists the authentication mechanism and the associated Active Directory, LDAP, and Delinea Directory account properties that must be set correctly. If a property is not set correctly, the user may not be able to log in.

Authentication mechanism	Required user account property	Active Directory/LDAP Properties tab	Delinea Directory Profile property
Password	Login Name and Suffix	User logon name on the Account tab	NA
Mobile Authenticator	Registered device	Not applicable	Not applicable
Phone call	Mobile phone number	Open the Telephones tab and set the Mobile field	Set the Mobile Number field
Text message (SMS) confirmation code	Mobile phone number	Open the Telephones tab and set the Mobile field	Set the Mobile Number field
Email confirmation code	Any valid email address	Open the General tab and set the E-mail field	Set the Email address field
Security question(s)	NA	NA	NA
OATH OTP client	NA	NA	NA

Before you enable a specific authentication factor, confirm that each account has current contact information or a currently registered—and make account changes a day before you enable the authentication policy for the accounts. *If the information needed for a user's authentication is not current in Privileged Access Service, the user will not be able to log in.*

If you need to modify a user's Active Directory or LDAP account, any changes you make are not immediately updated in Privileged Access Service. For example, it can take up to 24 hours for changes made in Active Directory Users and Computers to be incorporated into the Privileged Access Service.

By contrast, updates made to Delinea Directory accounts go into effect immediately.

Note: Users can set their Active Directory or LDAP account's mobile phone number from the profile tab. When users change their Active Directory or LDAP account's mobile phone number using the Admin Portal, the change goes into effect immediately.

Temporarily Suspend Multifactor Authentication

If the user's account information required for multifactor authentication is not set properly and it prevents the user from logging in, you can use the MFA Unlock command in Admin Portal to suspend multifactor authentication for 10 minutes–see "User Management Commands" on page 274. The user must still enter the correct user name and password and is still prompted to enter the additional authentication factor, however, the Privileged Access Service does not validate anything beyond the user name and password. Consequently, the user can, for example, enter any string of characters to fulfill the SMS confirmation code, and the Privileged Access Service accepts the entry.

To temporarily suspend multifactor authentication for a user:

1. Log in to Admin Portal.
2. Click **Access > Users**.
3. Right-click the account for the user who is locked out.
4. Select **MFA Unlock**

   The user has 10 minutes to log in.

Browser Cookies Associated with Authentication Policy Controls

When you enable authentication policy controls, Privileged Access Service leaves the following identity cookies in your users' browsers:

- After multifactor authentication: The Privileged Access Service leaves a cookie in the current browser after the user has successfully logged in to Admin Portal by using a multifactor authentication method.

  When the directory service finds this cookie, it does not prompt the user to provide an additional authentication method for subsequent logins. If you want to require authentication for subsequent logins, then ensure that you do NOT have an authentication rule using the Identity Cookie filter and specify the Default Profile for one that has the necessary authentication methods. See "Creating Authentication Rules" on page 281 for instructions on creating authentication controls.
- After IWA Authentication: The Privileged Access Service leaves a cookie in the current browser when the user has successfully logged in to the Admin Portal using Integrated Windows Authentication.

When the Privileged Access Service finds this cookie, it ignores the multifactor authentication requirements and lets a user open a web application from the Admin Portal that is set with the “Restrict app to clients within the Corporate IP range” policy regardless of their IP address (see Removing an application).

Users are required to provide multifactor authentication if the cookies are deleted or they use a different browser to log in.

Settings UI fields

You use the Admin Portal Settings page to configure the following Privileged Access Service options. Before you develop your Privileged Access Service deployment plan, review these options. Some of them may be necessary to support certain mobile devices (for example, the Apple Push Notification Service certificate for iOS devices) while others are optional (Account Customization and Exchange ActiveSync Server Settings).

Modifying a setting requires specific Admin Portal administrative rights.The third column lists the required rights. To learn more about the roles and rights required to make these changes see "Admin Portal Administrative Rights" on page 277.

Setting	Why you use this setting	Role or rights needed to modify these settings
Account Customization	Customize the Admin Portal login prompts and email messages to incorporate your organizations brand and logos. See "How to Customize the Admin and Login Window" on page 249.	Sysadmin role
Authentication Profiles	Define the required authentication mechanisms such as password, email confirmation code, mobile authenticator, etc. You use the authentication profile when you create your authentication rule or when you are configuring Server Suite authentication. See "Creating Authentication Profiles" on page 284	Sysadmin role
Admin Portal	Display the list of Delinea Connectors, configure Integrated Windows Authentication settings, and add or delete a Delinea Connector. See How to install a Delinea Connector.	Sysadmin role to modify all settings Register Connectors permission to add a connector
Corporate IP Range	Specify the public IP addresses you want to include within the corporate intranet. Privileged Access Service uses these addresses for Integrated Windows Authentication and application multifactor authentication. See "How to Set Corporate IP Ranges" on page 318	Sysadmin role

Setting	Why you use this setting	Role or rights needed to modify these settings
Directory Services	Add LDAP or Google as your directory service and view existing configured directory services. See "How to Add a Directory Service" on page 256.	Sysadmin role
Idle User Session Timeout	Enable a timeout and set the time period to log out inactive users from Admin Portal and Privileged Access Service Admin Portal. See "How to Configure Idle Session Timeout" on page 247.	Sysadmin role
Login suffix	Create a list of the login suffixes (the name that follows @ in the full user name) that users enter to log in to the Privileged Access Service Admin Portal and enroll devices. Users that do not have a login suffix in this list cannot log in to the portals or enroll a device. See "How to Use Login Suffixes" on page 236.	Sysadmin role
OATH Tokens	You can authenticate the Privileged Access Service using your existing third-party OATH tokens (for example, those generated by a YubiKey) by bulk uploading those tokens. Privileged Access Service uses those tokens to generate one-time passcodes (OTP) that users with enrolled devices can immediately use to log in to the Admin Portal. See "How to Configure OATH OTP" on page 347.	Sysadmin role
Partner Management	Allows you to add business partners so that you can share your Privileged Access Service with your partners. Partner federation is achieved through SAML, where your tenant serves as the host (the Service Provider in SAML terms), and your business partners access the tenant and its associated resources by passing a SAML token obtained from their Identity Provider (IDP). See "How to Set Up Business Partner Federation" on page 261.	Sysadmin role
Provisioning	Run application user provisioning synchronization, configure the provisioning report options, and specify daily synchronizations.	Sysadmin role
RADIUS Connections	Allows you to configure your RADIUS clients/servers. You can use the Delinea Connector as a RADIUS server for clients that support RADIUS authentication, such as VPNs. Additionally, you can configure RADIUS server settings to allow third-party RADIUS authentication. See "How to Configure Privileged Access Service for RADIUS" on page 323.	Sysadmin role

Setting	Why you use this setting	Role or rights needed to modify these settings
SafeNet KeySecure Configuration	Configure communication between the Privileged Access Service and the SafeNet KeySecure appliance if you want to use KeySecure to store Delinea privilege service account passwords.	Sysadmin role
Security Settings	Define security related settings such as securely capture users' passwords at login or enabling forgotten username self-service. See "How to Set Authentication Security Options" on page 296.	Sysadminrole
Server Suite Authentication	Add or select an authentication profile to use for multi-factor authentication on Delinea-managed Linux and UNIX computers. The authentication profile determines the authentication mechanism from which users can select how they are authenticated. See "Preparing Authentication Profiles" on page 352.	Sysadmin role
System Configuration	To configure a custom SMTP server to for outgoing mail service such as MFA challenges and self-service features. You can also choose to connect to the custom SMTP server using the Delinea Connector.	
Tenant URLs	Create a URL that is specific to your company so your users can easily remember the Privileged Access Service URL. Newly created URLs may take a few minutes to propagate. If you have users using FIDO2 authenticator(s), those users will need to log in with the new URL and re-activate their keys. See "Using FIDO2 Authenticators with a New Tenant URL" for more information. URL requirements: Always begin with an alphabet Maximum of 63 characters Can only contain alphabets, numbers, and dashes (-)	Sysadmin role

Navigating Your User Profile

The Admin Portal is your interface to the Privileged Access Service. The User Profile page in the portal allows you to configure your security settings, register devices that you want to use to access the Privileged Access Service, and see your Admin Portal activity.

Click **Profile** under your user name in the Admin Portal to access your user profile setings.

Using the Tabs

The Admin Portal Profile page has three tabs that you can use to do the following:

- **Security**: Allows you to change the password you use to log in to the Admin Portal, set up a security question, and set passcodes.
- **Devices**: List the devices you have registered in the Privileged Access Service.

See the following topics to register a device:

- "Registering an Android Device and Using the Delinea Application" on page 389
- "Registering an iOS Device and Using the Delinea Application" on page 395

- **Activity**: Display your Admin Portal activity log.

  See "Using Activity" on page 386 for more information.

Using Multi-Factor Authentication

Some organizations require you to provide multi-factor authentication when you log in to the Admin Portal, open an application, or register a device. Multi-factor authentication means you must enter your password plus provide another form of authentication to log in.

Privileged Access Service provides the following forms of authentication:

Authentication form	How you respond to complete the login
Mobile Authenticator	You can respond using either the Mobile Authenticator option in the Privileged Access Service application or your device's notification service. See "Using Mobile Authenticator" on the next page for further detail.
One-time-passcode (OTP)	
Email verification code	Access the relevant email account, open the email message, and click the link or manually enter the one-time code.
SMS verification code	Open the text message sent to the phone number indicated and either click the link or enter the code in the Admin Portal prompt. **Note**: The device must be connected to use the link.
Answer Security Question	Provide the answer to security question(s) you created and/or admin-defined question(s). You create your security question(s), select admin-defined question(s), and answer on the Accounts page in the Admin Portal–see "Specifying Security Question(s) and Answer(s)" on page 387
Phone call	Answer the call to the phone number indicated and follow the instructions.
FIDO2 Authenticator(s)	FIDO2 authenticator(s) are either on-device or external security keys that provide passwordless authentication. See "Using FIDO2 Authenticators" on page 367

Your IT administrator can enable all of them or just some of them. Your options are displayed in a drop-down list in the login prompt. Make your selection after you enter your password.

If you are required to user multifactor authentication, Privileged Access Service wait until you enter all challenges before giving the authentication response (pass or fail). For example, if you enter the wrong password for the first challenge, we will not send the authentication failure message until after you respond to the second challenge.

If you fail your first challenge and the second challenge is SMS, email, or phone call, the default configuration is that Privileged Access Service will not send the SMS/email or trigger the phone call. Your systems administrator can contact Delinea support to change this configuration.

Using Mobile Authenticator

The Privileged Access Service to send your device a notification when you choose Mobile Authenticator as your additional authentication method. You can use either the passcode or the Privileged Access Service application to complete the authentication process.

You must have the “Show notifications” device setting enabled to use your device notification for authentication. If this feature is not turned on, you use the Privileged Access Service application to authenticate with Mobile Authenticator.

Note: Do not select this option if you are logging in to an application from the same device.

When you select Mobile Authenticator as the additional authentication method, the notification is sent to your device after you enter your password. Responding to the notification is slightly different for Android and iOS devices.

Using the Privileged Access Service application as the Mobile Authenticator response

To use the Privileged Access Service application as the Mobile Authenticator response:

1. Open the Privileged Access Service application on the device.
2. Tap **Authenticate** at the bottom of the application.

   If your systems administrator has required finger print authentication (or PIN as a fallback option), then you must provide this information to access the mobile authenticator code.
3. Enter the code in the login prompt to complete authentication.

Using OTPs to Authenticate

You can use a one-time-passcode (OTP) to log in to the Admin Portal. You use a third party authenticator (like Google Authenticator) or the Cloud Client application to scan a Privileged Access Service generated QR code and configure the OTP. Delinea supports any authenticator app that support the OATH TOTP standard. Refer to https://openauthentication.org/about-oath/ for more information.

If an internet connection is not available, you can also use an offline OTP to log in to the Admin Portal. Users must log in first in online mode before an offline OTP profile is created.

Important: Your system administrator must enable these features before you can use them.

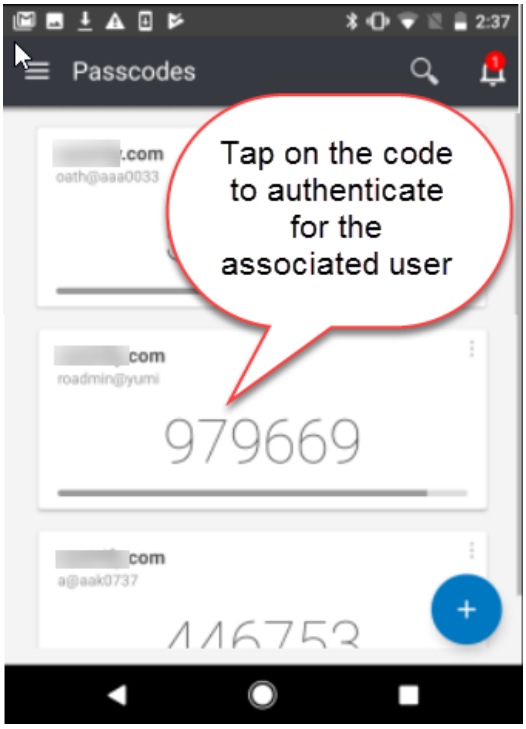
To setup a OTP

1. Log in to theAdmin Portal and navigate to **Access** > **Policies**.
2. Click on the policy you want to use for OAUTH OTP.
3. Click on **User Security** > **User Account Settings**.
4. Set **Enable users to configure an OAUTH OTP policy** to **Yes**.
5. Click **Security > OATH OTP Client**.

   The QR code displays.

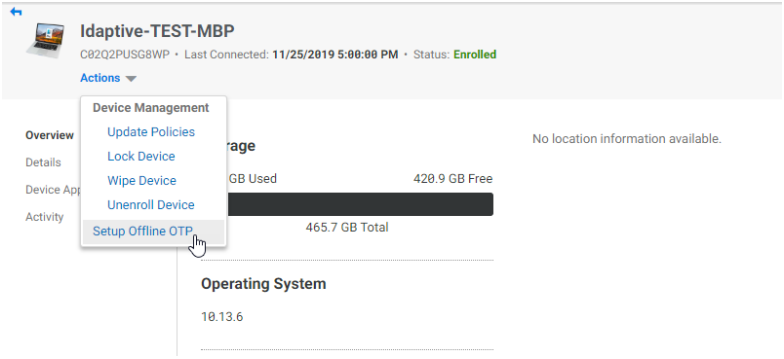
6. Use a third party authenticator application or the Cloud Client application on your device to scan the QR code.
7. A passcode is displayed on the third party authenticator application and on the **Passcodes** page of the Delinea application.

   You can now enter the passcode to log in to Privileged Access Service. This authentication works across tenants. On the **Passcodes** page of theDelinea application, you can tap the relevant code to silently send that code and authenticate for the relevant user/endpoint.



To setup an Offline OTP from the Admin Portal

1. Log in to theAdmin Portal > Profile.
2. Click **Passcodes**, then select **Offline OTP Client**.
3. Click **Actions > Setup Offline OTP**.



The QR code displays.

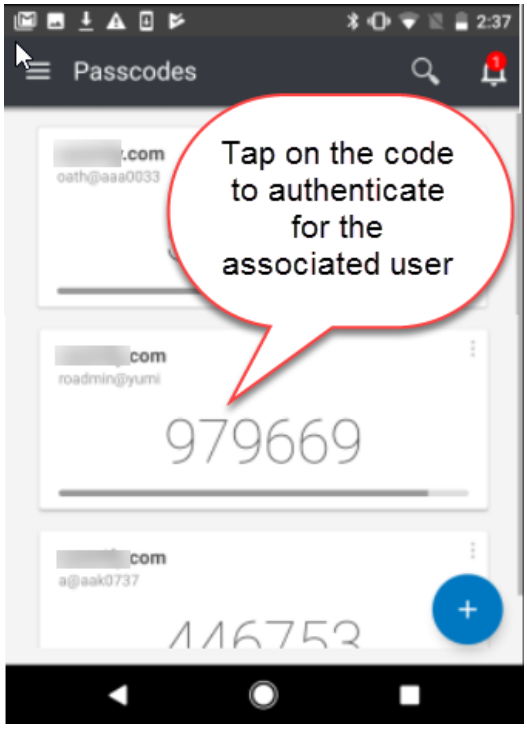
4. Use a third party authenticator application or the Cloud Client application on your device to scan the QR code.

   A passcode is displayed on the third party authenticator application and on the **Passcodes** page of the Delinea application.

5. Enter the verification code generated by the authenticator app, then click **Verify**.

   You can now enter the passcode to log in to Privileged Access Service when your device is offline.

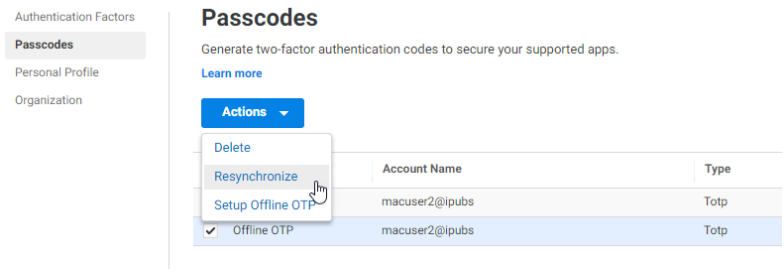
   On the **Passcodes** page of the Delinea mobile application, you can tap the relevant code to silently send that code and authenticate for the relevant user/endpoint.



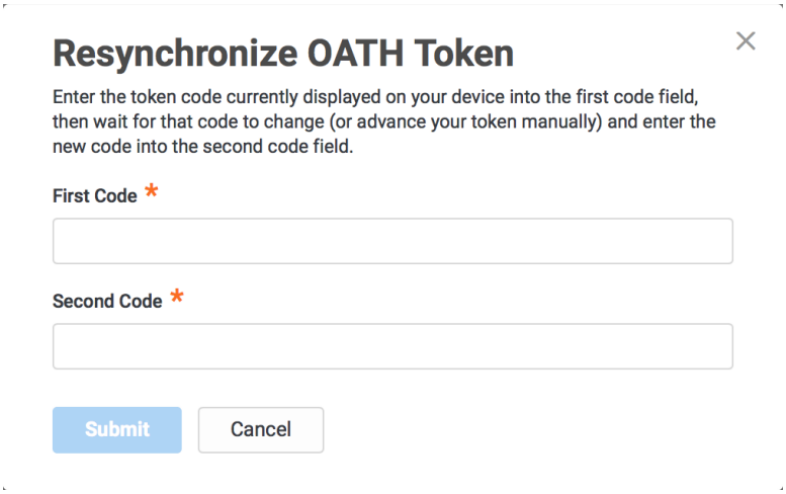
To resynchronize a OTP

If your OTP fails, you might need to resynchronize your OTP with the Privileged Access Service.

1. Log in to the Admin Portal > Profile.
2. Click **Passcodes**, then select the passcode that you need to resync.
3. Click **Actions > Resynchronize**.



4. Follow the directions in the Resynchronize OATH Token window, then click **Submit**.



Using FIDO2 Authenticators

FIDO2 is an authentication standard hosted by FIDO Alliance. This standard includes the Web Authentication ("WebAuthn") API, which is a specification written by the World Wide Web Consortium (W3C) and FIDO, with participation from additional third parties. The WebAuthn API is backward-compatible with Universal 2nd Factor (U2F) keys.

Delinea leverages the WebAuthn API to enable passwordless authentication to the Privileged Access Service using either on-device or external authenticators. On-device authenticators are biometric authenticators integrated into the device hardware. Popular examples are Mac Touch ID, Windows Hello, and fingerprint scanners. External authenticators are security keys that you plug into the device's USB port; for example, a YubiKey.

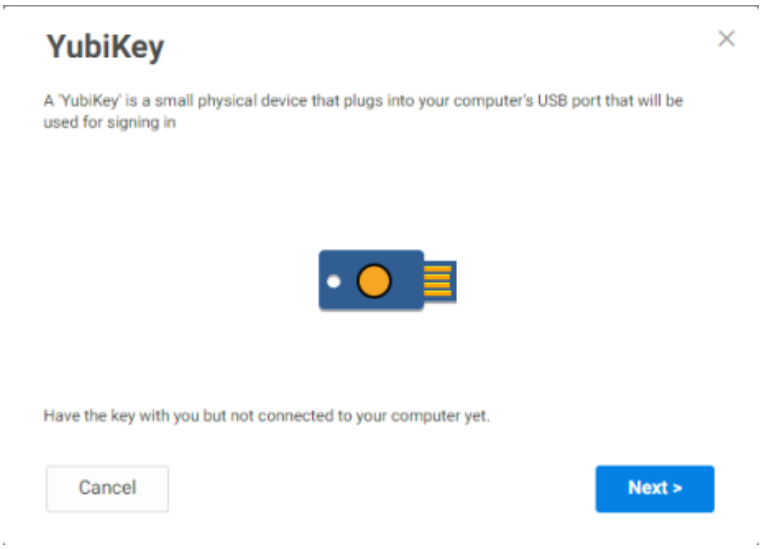
This feature requires prior configurations by your systems administrator.

To configure your FIDO2 Authenticator:

1. Log in to the Admin Portal > Profile page.
2. Click **Security** and then the button associated with the FIDO2 Authenticator name created by your systems administrator.
3. Add a FIDO2 Security Key (for example, a YubiKey), or an On-device Authenticator.

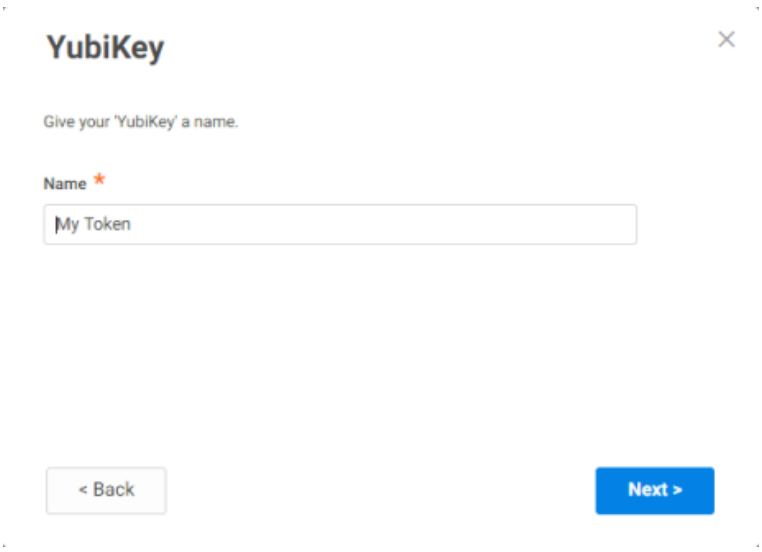
   Security Key

a. Click **Next** on the information screen.



b. Enter a name for your security token.

Most users will have only one token, but this name differentiates multiple tokens.



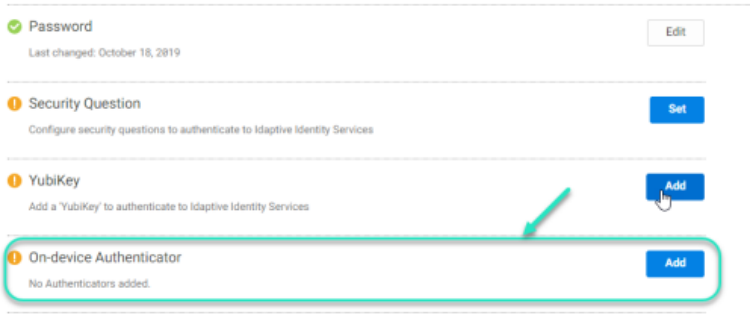
c. Click **Next**.

d. Insert your FIDO2 security key into your computer and follow the instructions on the screen.

You can now use your FIDO2 security key to authenticate to Privileged Access Service.

On-device Authenticator

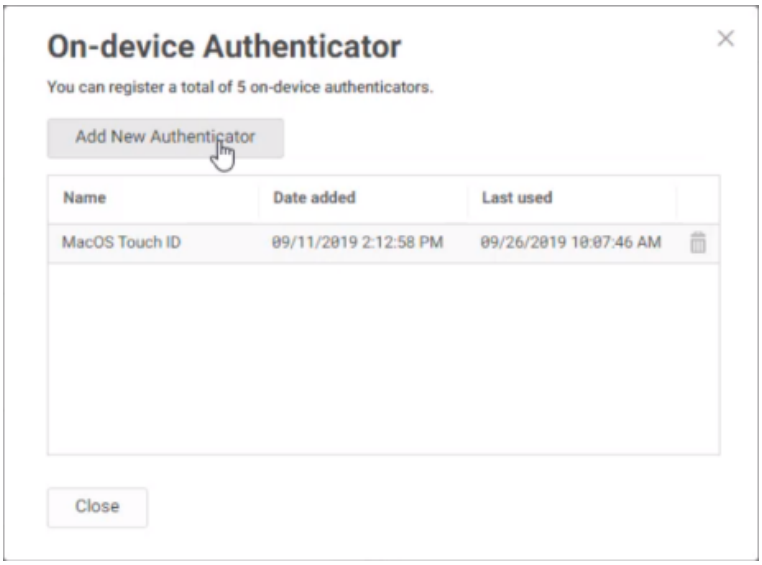
Click the **Add** button associated with the On-device Authenticator that you want to configure, then follow the on-screen instructions.



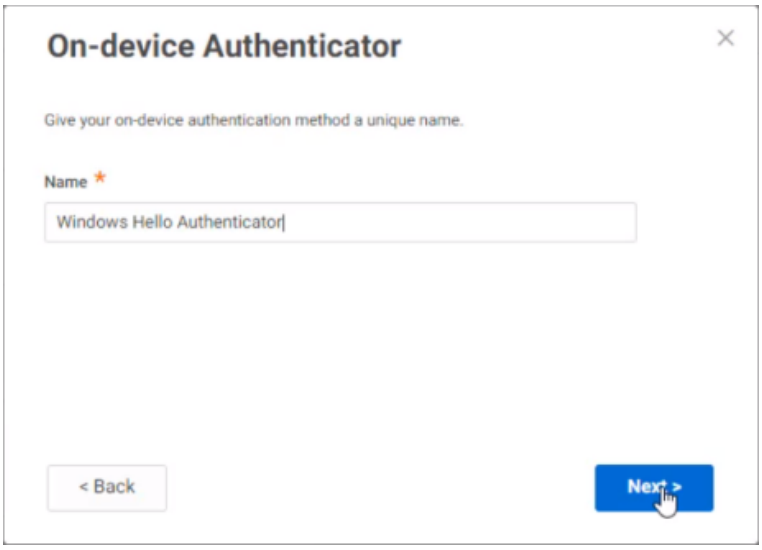
For example, the following procedures illustrate how to register a Windows Hello or Mac Touch ID authenticator. Other on-device authenticators have similar procedures.

Windows Hello

e. Click **Add New Authenticator**, then click **Next** on the following screen explaining what an on-device authenticator is.

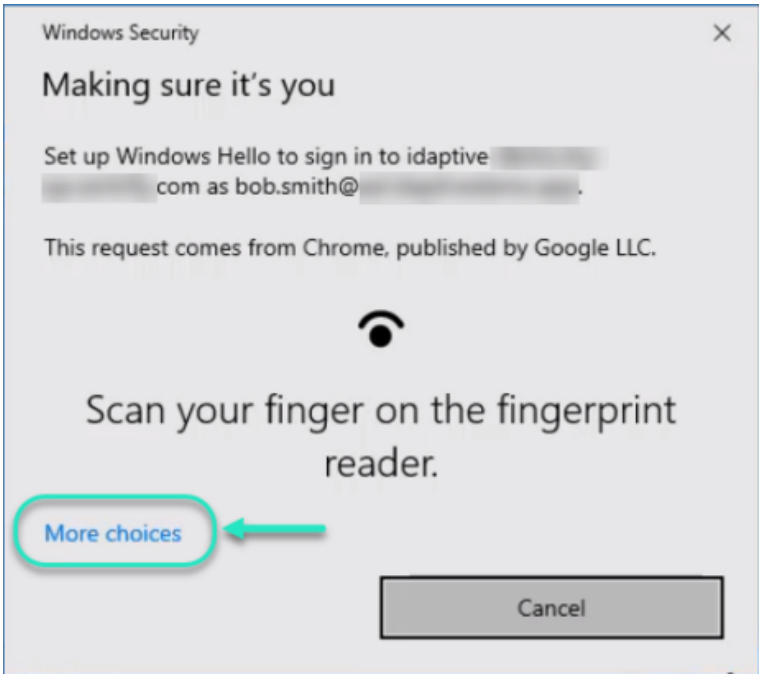


f. Enter a name for the authenticator, then click **Next**.



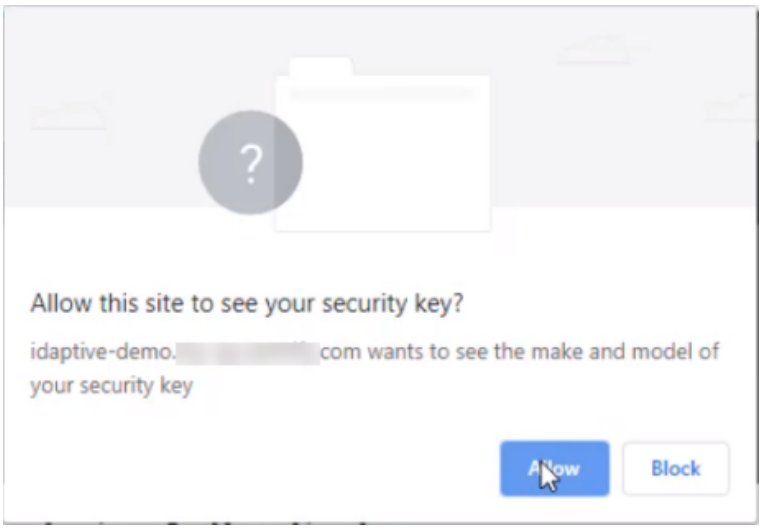
g. Interact with the authenticator at the prompt.

For Windows Hello, this could be a PIN, fingerprint, or security key. Click **More choices** if you want to change how you interact with Windows Hello.



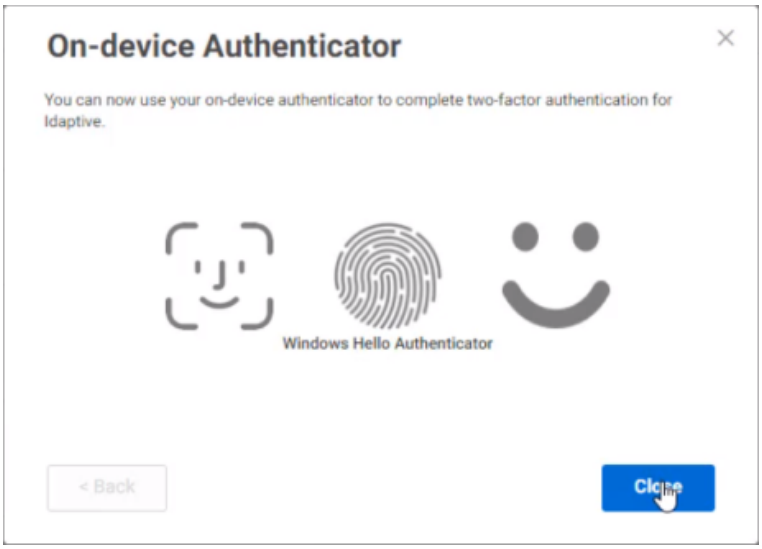
After interacting with the authenticator, a prompt appears asking for permission for the site to see your security key.

h. Click **Allow** to allow Delinea to see your security key (in this case, your fingerprint).



i. Enter any additional authentication that your administrator has required to complete the action, then click **Next**.

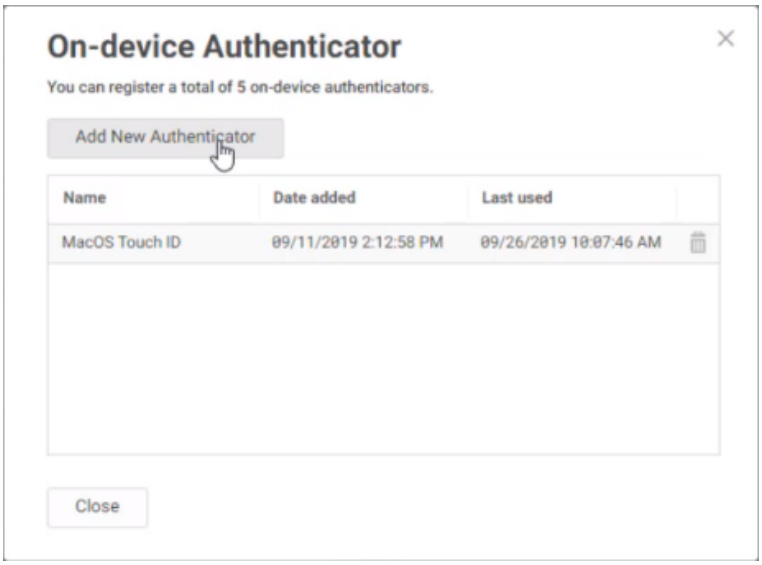
j. Click close on the final screen indicating that you can now use your on-device authenticator.



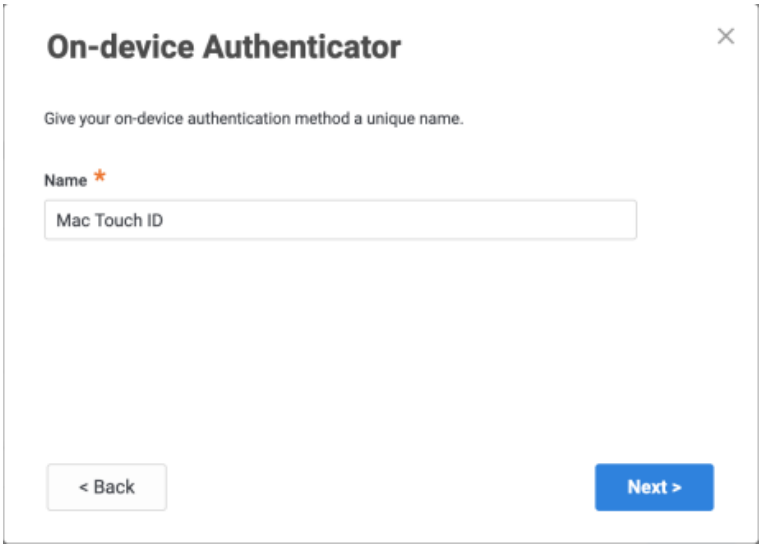
Mac Touch ID

k. Click **Add New Authenticator**, then click **Next** on the following screen explaining what an on-device authenticator is.

The lid on the Mac must be open for the browser to find the on-device authenticator.



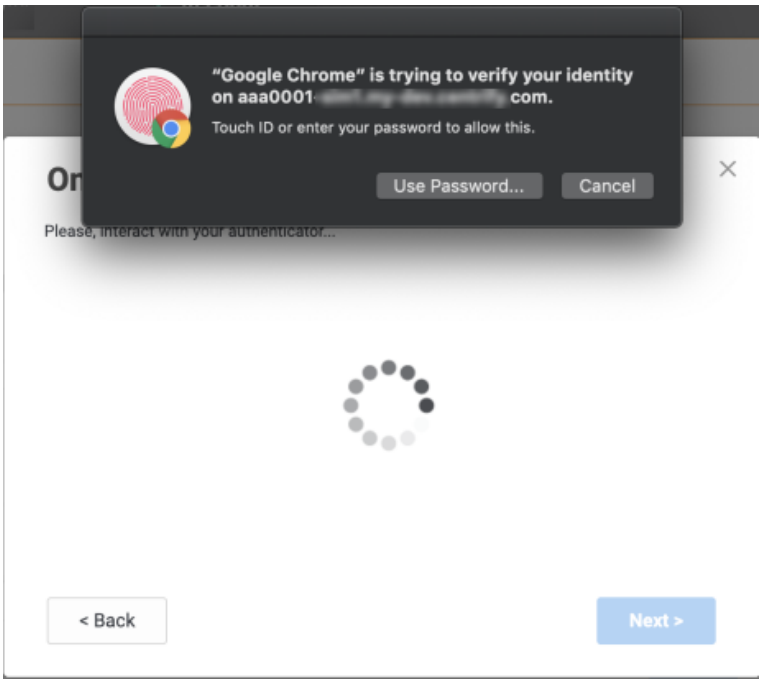
l. Enter a name for the authenticator, then click **Next**.



m. Scan your finger on the fingerprint reader at the prompt.

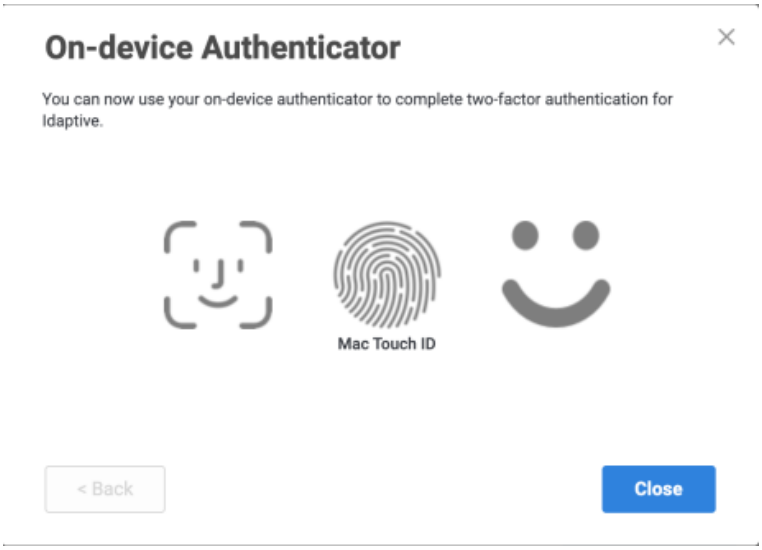
After scanning your finger, a prompt appears asking for permission for the site to verify your identity.

n. Click **Use Password...** to enter your password and allow the browser to verify your identity.



o. Enter any additional authentication that your administrator has required to complete the action, then click **Next**.

p. Click close on the final screen indicating that you can now use your on-device authenticator.



You may receive the following warning message: "Your current browser does not support <admin defined name> registration. Please contact your system administrator." The Web Authentication APIs used by FIDO2 authenticators are only supported on specified browsers. This browser support is controlled by the W3C and the FIDO Alliance and is unrelated to Privileged Access Service. Refer to https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/ for more information.

Integrate YubiKey HOTP with Delinea Hyper-scalable Privileged Access Service

The HOTP algorithm is an event-based OTP algorithm, where the changing factor is an event counter. HOTP uses a counter that increases each time a code is created and therefore, is time independent

This document is an end-to-end guide for integrating Yubikeys with the Delinea PAS using the OATH-HOTP.

Before you begin, you will need the following:

- #Company# PAS tenant. You can register a tenant here.
- Yubico personalization tool. Download the tool from here.
- Yubico Keys. Different keys can be compared here.

> **Note:** A Yubico Neo key is used in this document walk through.

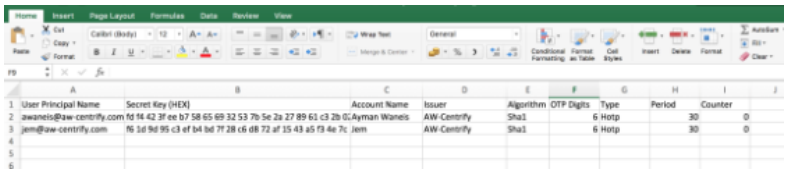
To setup your Yubikey:

1. Insert your Yubikey in your USB port. The Yubikey is a full-featured key with USB contacts. To learn more about its additional capabilities, seeYubiKey NEO
2. Configure the Yubikey.
   a. Start the Yubikey personalization tool.
   b. Select **OATH-HOTP**.
   c. Click the **Advanced** button.
   d. Ensure you are on the **OATH-HOTP** configuration tab.
   e. Ensure the Yubikey is inserted and can be read.
   f. Ensure **Configuration Slot 2** is selected.
   g. If **OATH Token Identifier** is already selected, deselect it.
   h. Select the **6 digits** option.
   i. Generate a secret key.
   j. Once the key is generated, highlight the key and copy it to a safe location. This key will be in a later step.
   k. Write the above configuration to the key.
   l. Confirm the configuration is written and no errors are displayed.

To Integrate Yubikey with Hyper-scalable PAS:

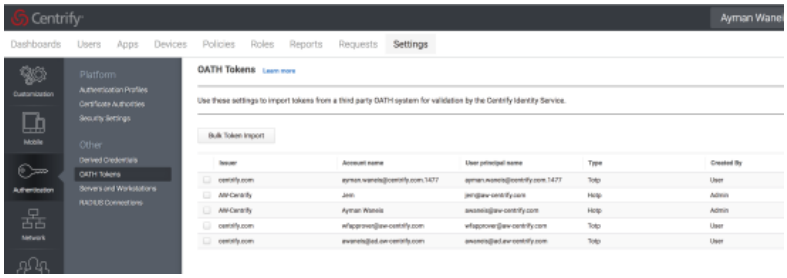
1. Log into the Delinea Portal as a Cloud Admin user and navigate to the **Settings** tab.
2. Select **Authentication** > **OATH Tokens**.
3. Click on **Bulk Token Import**. This opens the CSV file for the Yubikey token details.
4. Complete the bulk import spreadsheet as shown in the example below and save the file.

> **Note:** Ensure you paste the previously copied HEX key into the appropriate cell.



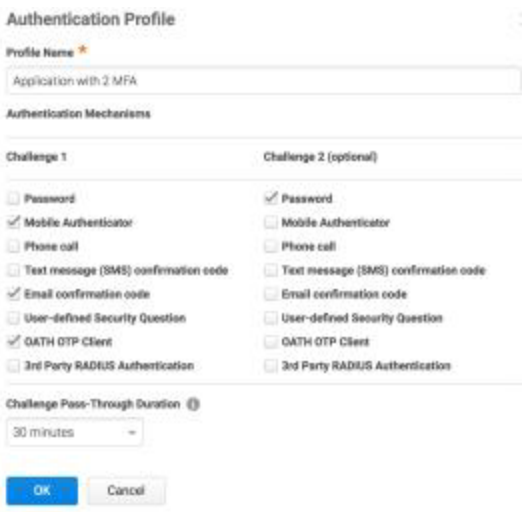
	A	B	C	D	E	F	G	H	I	J
1	User Principal Name	Secret Key (HEX)	Account Name	Issuer	Algorithm	OTP Digits	Type	Period	Counter	
2	awaneis@aw-centrify.com	fd f4 42 3f ee b7 58 65 69 32 53 7b 5e 2a 27 89 61 c3 2b 0	Ayman Waneis	AW-Centrify	Sha1	6	Hotp	30	0	
3	jem@aw-centrify.com	f6 1d 9d 95 c3 ef b4 bd 7f 28 c6 d8 72 af 15 43 a5 f3 4e 7c	jem	AW-Centrify	Sha1	6	Hotp	30	0	
4										
5										
6										

5. Browse to the saved spreadsheet and upload it.
6. Click **Next** to complete the key imports.
7. When you are done, you should see a configuration similar to this:



8. Create your custom Authentication Profile specifying the required options for the Multi-Factor Authentication profile.

   Note: Ensure you select **OATH OTP Client** on the either the 1st or 2nd challenge.



9. Enable the **Login Authentication** option.
10. Select a previously configured **Login Profile**.
11. Enable **OATH OTP** in the Policies Set.

Now that the configuration and integration is complete, users can use the Yubikey to login to Delinea Hyper-scalable Privileged Access Service.

To see your Yubikey integration:

1. Start the Delinea Portal.
2. Provide your login ID and click **Next** to go to the MFA login screen.
3. Touch the Yubikey for about 3 seconds, to generate the counter-based HOTP
4. You should be now be able to successfully log into your Delinea Portal environment.

For questions about how Delinea can help you consolidate user identities and solve the number 1 cause of all cyber-attacks, please contact us.

Logging into the Admin Portal From Your Device

Generally, you should use the Privileged Access Service application to log in to the Privileged Access Service from your device. However, there may be occasions when you want to log in to the Admin Portal from your device rather than use the Privileged Access Service application. To log in, you open your device native browser and enter the following URL:

https://cloud.centrify.com/home

After you are logged in, you can use the portal in the same way as you do from your computer browser. There are a few constraints:

- You must use the device native browser.
- Some applications cannot be opened. For example, you cannot open applications that require the browser extension. See "Launching Applications" below for more information.
- There may be a policy that prevents your from logging in.

Launching Applications

You can launch applications either from the Admin Portal or from the Delinea Browser Extension.

To launch an application from the Admin Portal

1. Log in to the Admin Portal and click **Apps > Web Apps**.
2. Click the box next to the application or right-click the application that you want to open.
3. From the Actions menu, click **Launch**.

To launch an application from the Delinea Browser Extension

1. Click the Delinea Browser Extension icon in your browser.
2. Find the application that you want to launch.

   You can use the drop-down menu to filter apps (for example, recently or frequently-used) or you can use the search field.
3. Click the application name in the list.

Installing the Browser Extension

Some applications require you to add the Privileged Access Service Browser Extension to your browser before you can open the application. You have two options for installing the browser extension:

- In the Admin Portal, click **here** in the banner or navigate to **Downloads** to install any browser extension.
- Launch any application that requires the Browser Extension and install it when prompted.

You only need to add the browser extension one time. Installation instructions are browser specific and are performed when you are logged in to the Admin Portal.

Chrome

1. In the Admin Portal click the **Apps** page.
2. Click **here** in the banner to initiate the download and installation of the browser extension or navigate to **Downloads** and click **Download** next to the Chrome extension.
3. The browser opens a new tab to download and install the browser extension.
4. Click **Continue** in response to the prompt “Are you sure you want to continue?” at the bottom of the window.

   The browser downloads the extension for Chrome.
5. Click **Add**.

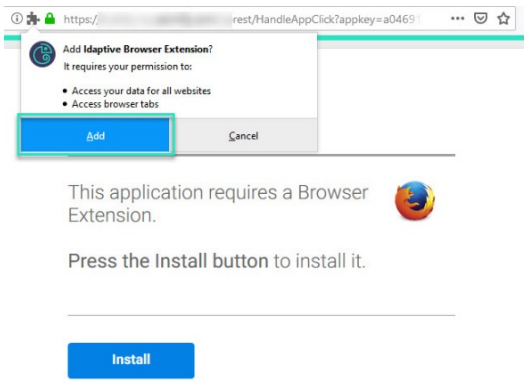
   This installs the extension in Chrome.
6. Close the tab used to download and install the extension.

   You are returned to the Admin Portal Apps screen. You can now open all applications that require the browser extension.

Firefox

1. In the Admin Portal click the **Apps** page.
2. Click **here** in the banner to initiate the download and installation of the browser extension or navigate to **Downloads** and click **Download** next to the Firefox extension.
3. Click **Allow** in the Firefox pop up window.

   Firefox downloads the extension.
4. Click **Install**.
5. Click **Add**.



6. Click **Restart Now**.
7. Restart your browser.

The browser extension is installed.

Note: Mozilla has discontinued side loading extensions as of Firefox 73; you will no longer be able to install extensions by placing extensions in the extensions folder.

Microsoft Edge

1. In the Admin Portal click the **Apps** page.
2. Click **here** in the banner to initiate the download and installation of the browser extension or navigate to **Downloads** and click **Download** next to the Microsoft Edge extension.
3. The browser opens a new tab to download and install the browser extension.
4. Click **Download** in response to the download window.

   The browser downloads the extension for Microsoft Edge.
5. Extract the contents of the zip file.
6. Close the tab used to download and install the extension and go to edge://extensions/or go use the **Extensions** menu option.

   Enable **Developer mode**, located at the bottom left of the page.
7. Click **Load unpacked** and select the unzipped folder.

   Click **Details** on the extension that was just added to expand the Advanced Section.
8. Click **Extension options**.
9. Update the **Portal Hostname** with your Delinea installation hostname and click **Save**.

   Note: The Extension options window won't automatically close after the save operation is complete, so you'll need to close it manually.

   You can now open all applications that require the browser extension.

Internet Explorer

1. In the Admin Portal click the **Apps** page.
2. Click **here** in the banner to initiate the download and installation of the browser extension or navigate to **Downloads** and click **Download** next to the Internet Explorer extension.
3. Click **Run** in the pop up window.
4. Click **Next** in the Privileged Access Service Browser Extension Setup Wizard to proceed.

   Continue responding to the prompts.
5. Click **Close** to exit the wizard.
6. Close the browser tab used by the wizard.
7. Click the **Tools** menu in the Internet Explorer's tool bar.
8. Click **Manage add-ons**.
9. In the pop-up window, click the Privileged Access Service Browser Extension and click the **Enable** button.
10. Click **Close**.

11. Restart Internet Explorer.

    You can now open all applications that require the browser extension.

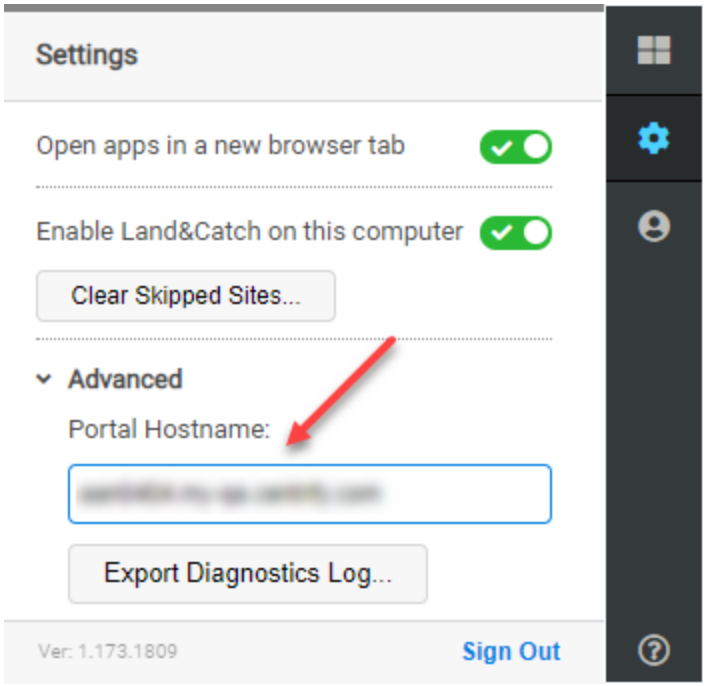
Using the Delinea Browser Extension

You can use the Delinea Browser Extension to change your portal hostname or export the diagnostics log file.

To change your portal hostname:

The portal hostname does not typically have to change from its default value; however, if your company uses multiple tenants, your system administrator might request that you change the portal hostname to an appropriate value for your tenant.

1. Click the Delinea Browser Extension icon in your browser, then click the gear icon to go to the Settings tab.
2. Expand Advanced, then enter the name of your tenant in the Portal Hostname field.

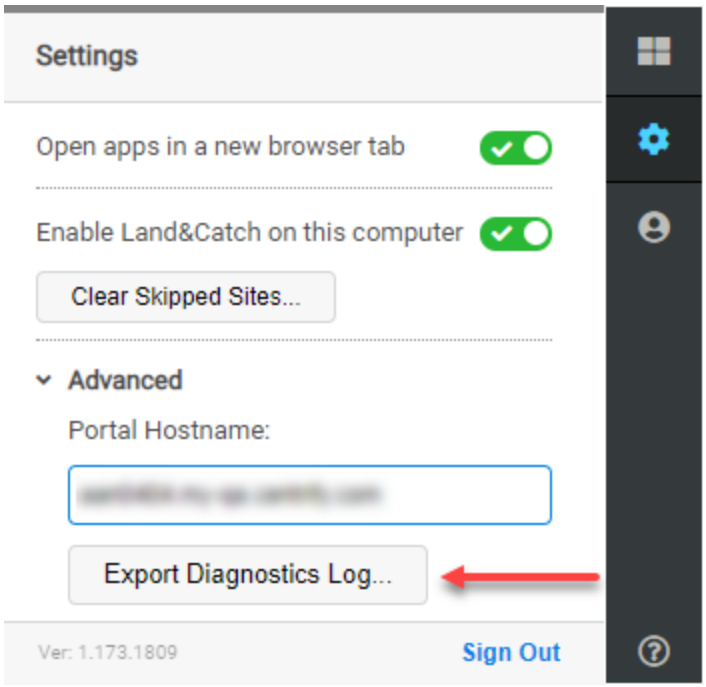


   The portal hostname typically takes the format <tenant>.Centrify.com. You will see a red X in the field for invalid hostnames, and a green checkmark after entering a valid hostname.

To export the diagnostics log file:

Your system administrator might need you to export the Delinea Browser Extension diagnostics log to assist in troubleshooting.

1. Click the Delinea Browser Extension icon in your browser, then click the gear icon to go to the Settings tab.
2. Expand **Advanced**, then click **Export Diagnostics Log**.



The log file is downloaded to your browser's default download location. The file name takes the format BElog-YYYYMMDD-HHMMSS.bin.

Requesting Access to an Application

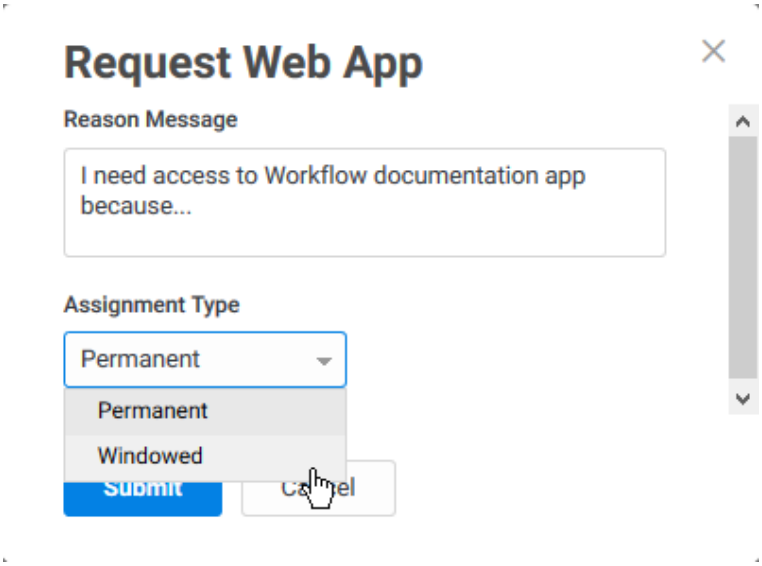
Any user who has an account in the Privileged Access Service can request access to applications that the administrator has configured with a “request and approval” work flow. No special privileges are required to make requests or approve requests.

To request access to an application

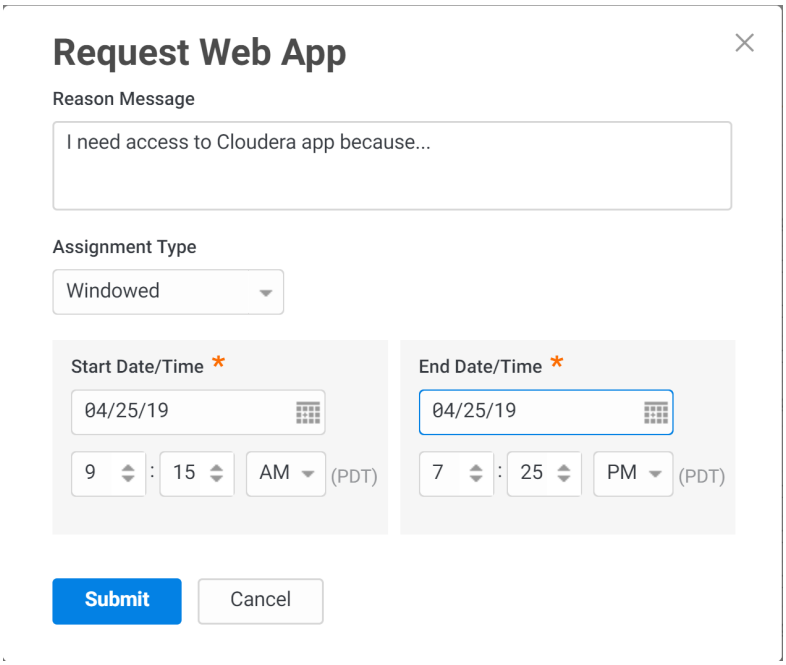
1. Log on to the Admin Portal.
2. Click **Apps > Add Web Apps**.
3. Type a search string to find the application of interest in the catalog, then right-click or select the check box next to the application.
4. Select **Request Launch** from the Actions menu.

   Only applications with workflow enabled display a Request Launch option.
5. Select either **Permanent** or **Windowed** in the Assignment Type drop-down menu.
   - Permanent - if the request is granted, the user will have access to the app for an indefinite time period, or until it is revoked by an administrator.
   - Windowed - if the request is granted, the user will have access to the app for the specified window, or until it

is revoked by an administrator.



6. (Optional) Select the start and end date and time if the request is for a windowed assignment type.



7. Type the business reason for requesting access to the application, then click **Submit** to continue.
8. Click **Close** to close the App Catalog.

   An email notification of your request is sent directly to the designated approver. You can click the Requests tab to see the status of your request. You will also receive an email notification when you request is approved or rejected. If your request was approved, the email will include a link to open the Admin Portal.

Viewing Request Status and History

You will only see the Requests tab if you have made a request or approved a request. After you have made or responded to at least one request, you can click the Requests tab to view the status of requests and the history of request activity.

The list of requests includes the following information:

- **Description** provides a brief summary of the request indicating the type of access or application requested.
- **Status** displays the current status of the request as Pending, Approved, Rejected, or Failed.

  You can review the request details to see the reason the request failed. For example, a request might fail if the email address for the approver or requester is invalid. A failed request might also indicate that the time allowed for taking the requested action has expired. For example, assume the request was for permission to use the root account to log on to a resource and the request was approved with a duration of 60 minutes. If the requester did not log on within 60 minutes of the request approval, the request status will display **Failed**.
- **Posted** displays the date and time of the most recent activity for each request.
- **Approver** displays the user or role designated for approving access requests if the approval is pending or the specific user who approved or rejected the request if the request has been resolved.
- **Requester** displays the user who submitted the request.
- **Latest Log Entry** displays the most recent information recorded for the request.

Viewing Request Details

You will only see the Requests tab if you have made a request or approved a request. After you have made or responded to at least one request, you can click the Requests tab to view the status of requests and the history of request activity.

If you are an approver, you can also go directly to Request Details by clicking the link in the email notifying you of the request.

Regardless of the entry point for viewing request details, the request information table displays details appropriate for the current state of the request. For example, you might see the following information:

- Posted displays the date and time of the most recent activity for each request.
- Description provides a brief summary of the request indicating the type of access or application requested.
- Requester displays the user who submitted the request.
- Requesters Reason displays the business reason provided by the user who submitted the request.
- Approver displays the user or role designated for approving access requests if the approval is pending or the specific user who approved or rejected the request if the request has been resolved.
- Status displays the current status of the request as Pending, Approved, Rejected, or Failed.

  Depending on the status of the request, you might see the reason the request was rejected or the reason why the request failed.

Using Devices

The Devices page lists all the devices you have registered in the Privileged Access Service and lets you send commands to the devices. The Devices page is blank until you register a device.

Not all companies use the Privileged Access Service for device registration. Contact your IT department to determine whether or not you should register your mobile devices.

Adding a Device

You add a device by installing the Delinea application on the device and then use this application to register the device in the Privileged Access Service. After you register the device, it is listed on the Admin Portal > Profile Devices page and remains registered until you or your IT administrator unregisters it.

Installing the Delinea Mobile Application

The easiest way to install the Delinea application to your device is to click **Add Devices** on the Devices page and then select a method.

You can install the Delinea application using the following methods (available methods are configured by your systems administrator):

- Send an email to the device. The email message contains a link you tap to proceed. See "Using an Email Message" below.
- Use the camera on your device and a QR code reader application. See "Using the QR Code" on the next page for further detail.

The Google Play and App Store links are provided if you want to review the application description in the catalog before installing it on the device. You can also use them to download the application. You must have an Google Play or Apple App Store account to use these options.

We support the following versions:

- iOS version 10.0 or later
- Android 4.2 or later

Using an Email Message

You can send an email to the device to download the Delinea application to your device and then install it from the Downloads folder.

To initiate device registration using an email message:

1. Open the **Admin Portal > Profile** page, click **Devices**, and **Add Devices**.

   This opens the Add Devices pop up window.
2. In the **Send registration link via:** area, confirm the email address then click **Send**.

   The email is sent.
3. On the device, open the email application.
4. Tap the message.

5. Authorize application download.

   On an Android device, tap **OK** to allow download of the file. This downloads the application file to your Downloads folder.

   On an iOS device, tap **Open** to open the application page in the Apple App Store and tap **Install**. This downloads and installs the application onyour home screen. Skip the next step and go to "Registering an iOS Device and Using the Delinea Application" on page 395 to complete registration.

6. Android devices only: Open the Downloads folder on the device and tap the Delinea application file just downloaded.

   This initiates application installation. Go to "Registering an Android Device and Using the Delinea Application" on page 389 to complete registration.

Using the QR Code

You must have a QR code reader application to download the Delinea application using the QR code.

Many devices come equipped with a QR code reader application. If your device does not have one by default, there are many free apps you can install from Google Play or the Apple Apps Store.

To install the Delinea application by using the QR code:

1. Open the **Admin Portal > Profile** page, click **Devices** and then click **Add Devices**.
2. On the device, use the camera to scan the QR code.
3. Authorize application download.
   a. On an Android device, tap Go to Website and then tap **OK** to allow download of the file. This downloads the application file to your Downloads folder.
   b. On an iOS device, tap **Install**. This downloads and installs the application on your home screen. Skip the next step and go to"Registering an iOS Device and Using the Delinea Application" on page 395 to complete the registration phase.
4. Android devices only: Open the Downloads folder on the device and tap the Delinea application file just downloaded.

   This initiates application installation. Go to "Registering an Android Device and Using the Delinea Application" on page 389 to complete registration.

Using Apple Device Registration

The Apple Device Enrollment Program is a service provided by Apple. It is designed to help businesses and education institutions easily deploy and manage iPads, iPhones, and Macs. It provides a fast, streamlined way to deploy company owned iPad and iPhone devices and Mac computers that your IT department purchased directly from Apple.

If you have a device assigned to the Apple Device Enrollment Program (DEP) registering the device is a two-part process:

- First, you register the device in the Apple DEP program.
- Second, you use the Delinea application to register the device in the Privileged Access Service.

The first procedure depends upon how your IT department configured the device. However, it does have the following basic steps:

1. Set up the device communications.

   The device will need to connect to the Apple server. Your IT department will provide the information you need.

2. Enter your login user name and password.

   This may be the user name and password you use to log in to your network or another set of credentials. Your IT department will provide these to you too.

3. Perform the initial configuration tasks.

   These vary depending upon your organization's security policies and can include prompts, for example, to setup a passcode, enable or disable location tracking, or set up Siri.

After you have completed the initial configuration tasks, the Delinea application and the Company Apps applications are automatically installed on your home screen. To perform the second registration piece—registering the device in the Privileged Access Service— see "Registering an iOS Device and Using the Delinea Application" on page 395.

Viewing Your Device Information

When you open the **Devices** tab, the screen lists all of the devices that you have registered in the Privileged Access Service, including devices that have been unregistered.

A device can have the following statuses:

- **Registered**: The device is registered and in communication with the Privileged Access Service.
- **Unregistered**: The device was registered at one time but has since been unregistered from the Privileged Access Service.
- **Unreachable**: The device has not communicated with the Privileged Access Service for a period of time. That period of time is set by your IT administrator.
- **Registering**: The device is in the process of registering with the Privileged Access Service. This is typically a short-term state.

The map shows the location of all the devices you have at one time been registered. For unreachable devices, the map shows the last known location. Click on the device's arrow to center the focus on that device.

The map device locations are only shown if your organization is using the Privileged Access Service for mobile device management and you have enabled device tracking on the device and in the Privileged Access Service Admin Portal.

By default, location tracking is enabled in the Privileged Access Service Admin Portal.

In the Delinea application on iOS devices, location tracking uses the significant-change location service which, unlike the GPS location tracking, is very battery friendly. It is not perpetually trying to determine the device location. Note that the Apple Location icon does not differentiate between the different types of location services.

Similarly, the Delinea application for Android is configured for low power consumption. Open Location in the device Settings to see the battery use for the Delinea application.

If the location does not seem correct, click the Find Now button to ensure that you have the most recent GPS location data. You may need to reload the browser page to display a location change.

Sending Commands to Devices

The Privileged Access Service provides self-service commands you can send to the device. Send commands by doing one of the following in the Privileged Access Service Admin Portal > Profile:

- Right-click the device in the **Devices** screen.

  The Privileged Access Service Admin Portal displays a drop-down list with the commands.

The available commands depend upon the following:

- The type of device you have registered.
- The device policies that your IT administrator has enabled for you.

The following table lists all of the Privileged Access Service commands for all devices. If the command is not displayed in the pop up menu, it is not available for that device.

Command	Purpose
Lock Client App	Locks the Delinea application on the device. This command is only available on iOS and Android devices.
Reset Client App PIN	Resets the passcode for the Delinea application on the device. This command is useful when you forget your passcode. This command is only available on iOS and Android devices.
Email Device Log	Sends the device log file in the device to an email address. You specify the email address when you click the command. You can also set an option to send the log file when the device is on Wi-Fi only.

Using Activity

The Activity page lists the date and time of actions performed and commands sent to your devices by you and the system administrator. The actions include the following:

- Logged in and logged out
- Launched an application
- Registered a device
- Changed your password
- Failed in an attempt to log in

See "Sending Commands to Devices" above for the description of the commands that can be sent to your devices.

You can sort the actions by date and time or detail. For example, click **When** to sort the items by date and time in alternating ascending or descending numeric order. Similarly, click **Detail** to sort by the action type in alternating ascending or descending alphabetic order.

To find a specific activity or set of activities, enter the keyword in the Search box. The Admin Portal filters the list as you enter each character. To return to the full list, delete the search text.

Specifying Security Question(s) and Answer(s)

Some organizations require multifactor authentication when you log in to the Admin Portal or an application from the Admin Portal. If your organization requires multifactor authentication and allows you to use a question and answer as an authentication method, you are prompted to specify the question and answer when you log in to the Admin Portal or after the system administrator configures the policy.

To set and change your security question(s) and answer(s):

1. Log in to the Admin Portal > Profile.
2. Click the **Security** page and then click **Security Questions**.
3. Specify/Enter the question(s) and answer(s).

   The number of questions available is configured by your system administrator. The admin-defined security questions are available in a drop-down list. User-defined security questions are free form text.

   The answer can be multiple words. It is case sensitive and the spaces you enter must be entered when you log in.

   Note: Leading and trailing spaces are stripped off. Otherwise, you must enter the answer exactly as specified in the New Answer text box.

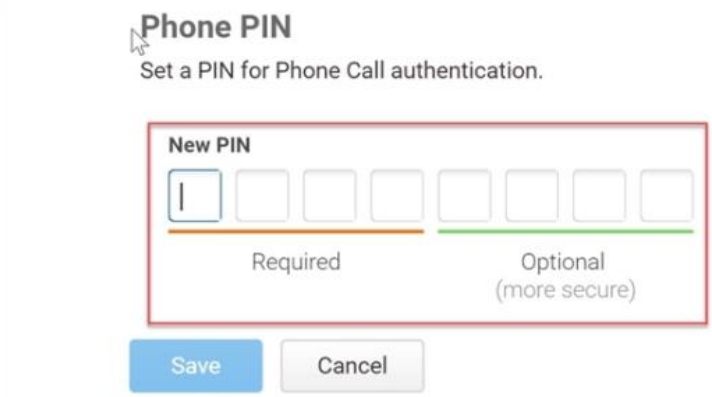
4. Click **Save**.

Specifying a Phone PIN

If your systems administrator asks you to create a PIN to authenticate using the phone call mechanism, then proceed with these instructions. Your systems administrator must first enable this feature before you can authenticate using the phone call mechanism.

To specify a phone PIN:

1. Log in to the Admin Portal.
2. Click **Profile > Security** and then click the Phone PIN area to configure.
3. Specify your PIN.



4. Click **Save**.

Changing Your Network Login Password

If you have a Privileged Access Service User account, changing your password changes the password you use to open the Admin Portal and to register devices. If you have an Active Directory User account, this also changes the password you use to log in to your company account when you start up your computer.

Your IT administrator controls whether or not you can change your password.

If you have an Active Directory User account, you may need to change other passwords as well. For example, if you log in to Outlook with the same account, you'll need to change that login password to match. Confirm with your IT staff regarding other passwords you may need to change after you change your Active Directory User account password in the Admin Portal.

To change your network log in password using Admin Portal:

1. Log in to the Admin Portal.
2. Click **Profile** from the user name dropdown menu in the upper right corner of the Admin Portal.
3. Click **Security > Password**.
4. Enter your current password.
5. Enter the new password.
6. Reenter the new password to confirm.
7. Click **Save**.

You can also change the password using your registered device. See "Changing Your Active Directory or Delinea Application Password" on page 397.

Managing Authentication Keys

You can use the Privileged Access Service Admin Portal to get the one-time passcode (either by scanning an external source's QR code or entering the authentication key information manually). You then can use the passcode to log in to the relevant application or website.

- Android devices: See "Registering an Android Device and Using the Delinea Application" below for information on scanning QR code using your Android device.
- iOS devices: See "Using Privileged Access Service as an Authenticator" on page 398 for information on scanning QR code using your iOS device.

To enter the authentication key information manually on your computer:

1. Log in to the Privileged Access Service Admin Portal on your computer and locate the dropdown menu under your log in name in the upper right corner of the Admin Portal.
2. Click **Profile > Security Passcodes > Add Accounts**.
3. Enter the information provided by the application or website.
4. Click **Save**.

   The newly-created passcode is available in the Passcodes window on your registered device.

Registering an Android Device and Using the Delinea Application

You register your device in the Privileged Access Service using the Delinea application. If you have not installed the Delinea application, see "Using Devices" on page 383 then return here to complete device registration.

Your organization may also configure mobile device policy profiles. The profiles set system preferences that configure communications with your corporate network and may impose some restrictions on your use of some device features.

Registering Android devices

You use the Delinea application to register your device. If you have not yet installed the Delinea application on your device, go to "Using Devices" on page 383 for the instructions.

To register the device:

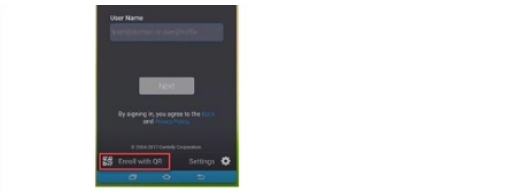
1. If the Delinea application is not already running, open **Apps** on the device and tap the icon.
2. Enter your user name and password.

   Your IT administrator will provide you with the user name and password you should use.

   Note: You may choose other authentication methods using the **Authentication Method** dropdown such as Mobile Authenticator or OATH OTP Client.

3. (Contingent upon configuration) If your systems administrator has enabled the feature, you can register your device without entering your user name and password. Do the following:
   a. Tap **Register with QR**.

      The scanning tool opens.



b. Scan the QR code on **Admin Portal > Profile > Devices > Add Devices**.

c. Click **Proceed** on the device browser.

The device registers.

Using the Delinea Application

You use the Delinea application to view and manage system resources from your device. Also, if your IT department requires a one time passcode to log in to the Admin Portal, you use the Delinea application to generate the one-time passcode.

Securing Your Delinea Application

You can secure your Delinea application using a PIN, fingerprint, or Near Field Communication (NFC) tag. The fingerprint option is only supported on iOS / Android devices that have the fingerprint recognition functionality.

To secure your Delinea application:

1. Tap the Delinea application on your device.
2. Tap the menu icon in the upper left corner and click **Lock App**.
3. Enter a PIN as your primary access method.
4. (Optional if enabled) Register your fingerprint or NFC tag as alternative access methods.

   If fingerprint recognition is available on your device, then we direct you to the device fingerprint registration window.

   If you have an NFC tag, then enter your PIN to register the tag. You can register a maximum of 5 tags.
5. Tap the menu icon in the upper left corner and enable the feature using the **Lock App** button.

   The setting defined by your system administrator overrides your setting here.
6. (Optional if enabled) Tap **Auto-Lock** and configure how long you want the Delinea application to be inactive before it automatically locks up.

   You will now be prompted to use one of the configured methods (PIN, fingerprint, or NFC tag) to access the Delinea application.

Changing Your Active Directory or Delinea Application Password

If you have a Privileged Access Service User account, changing your password changes the password you use to open the Delinea application and to register devices. If you have an Active Directory User account, this also changes the password you use to log in to your company account when you start up your computer.

Your IT administrator controls whether or not you can change your password.

If you have an Active Directory User account, you may need to change other passwords as well. For example, if you log in to Outlook with the same account, you'll need to change that login password to match. Confirm with your IT staff regarding other passwords you may need to change after you change your Active Directory User account password in the Delinea application.

To change your account password on your device:

1. Tap the Delinea application on your device.
2. Tap **Settings > Change Password**.
3. Enter your current and new passwords.
4. Tap **Save**.

Checking Out an Account Password

Delinea lets you securely store user name and password combinations in the Privileged Access Service for local accounts. You can use those accounts to log on securely to the servers, switches, and routers you identify as *Systems, Domains, and Databases*.

In addition, you can check out passwords for Delinea-managed local administrator accounts for registered devices. You can either show the password or copy it to the clipboard, then use it to perform operations that require admin rights.

Checking out an account password requires the following:

- Appropriate administrative rights on the Delinea identity platform.
- Existing access to Delinea privilege service (for Systems accounts).
- The device must be registered in the Privileged Access Service.
- Your authentication mechanisms must be configured for the Delinea application – see "Securing Your Delinea Application" on the previous page.

Account Types You Can Check Out

The following are account types you can check out passwords for:

- Tap **Systems** on the Delinea application to see available systems and check out the password for a stored account.
- Tap **Domains** on the Delinea application to see available domains and check out the password for a stored domain.
- Tap **Databases** on the Delinea application to see available domains and check out the password for domains.

> **Note:** You need view and checkout permission to check out a system, domain, or database password.

When you check out a password, it remains checked out until either you check it back in or the checkout time expires. The maximum check out time is configured by your admin through policy; however, you can extend the checkout time for a password that is currently checked out. When you extend the time, it is reset to the maximum check out time.

Checking Out a Password

For detailed steps on how to check out a password, see "Checking Out an Account Password" on the previous page. You can view these operations in the activity stream of the resource in portal. To do this: navigate to a resource, select the resource and choose the **Activity** tab.

Using Privileged Access Service as an Authenticator

You can use the Privileged Access Service Admin Portal >Profile > Device page to get the one-time passcode (either by scanning an external source's QR code or entering the authentication key information manually). You then can use the passcode to log in to the relevant application or website.

To scan a QR code

To scan a QR code, you must use the Privileged Access Service Admin Portal application on an registered mobile device.

1. Log in to the Privileged Access Service application on your mobile device.
2. Tap **Passcodes**.

   The Authentication window shows any existing passcodes.
3. Tap the plus icon (**+**) then tap **Scan QR Code**.
4. Scan the external source's QR code.

   The Passcodes window shows the newly generated passcode. The newly added authentication account is also added to the Passcodes page in the Accounts section of the Admin Portal.

To enter the authentication key information manually on your mobile device

To enter the authentication key information manually, you can use the Privileged Access Service Admin Portal on your mobile device or computer. See "Managing Authentication Keys" on page 388 for information on entering the authentication key information manually using your computer.

1. Log in to the Privileged Access Service application on your mobile device.
2. Tap **Passcodes**.

   The Passcodes window shows any existing passcodes.
3. Tap the plus icon (**+**) then tap **Enter Authentication Key**.
4. Enter the information provided by the application or website.
5. Tap **Save**.

   The Passcodes window shows the newly generated passcode. The newly added authentication account is also added to the Passcodes page in the Accounts section of the Admin Portal.

Using the Settings Screen

The Settings screen contains device configuration information such as default browser settings, authentication settings, and other useful information.

Login Settings

Contains the Privileged Access Service service URL.

Do not change this setting unless specifically instructed to by your IT department. If the URL is wrong, you cannot use the Privileged Access Service.

Authentication

Lets you configure the following:

- Mobile authenticator – See "Using Multi-Factor Authentication" on page 363
- Application lock settings

  Allows you to configure lock options for the Delinea application on your device. Configurations made by the system administrator override your user configuration.

  See "Securing Your Delinea Application" on page 390 for more information.
- Change Password

  Allows you to change your Active Directory or Privileged Access Service account password. See "Changing Your Network Login Password" on page 388.

Browser Settings

You use this option to set your default browser and clear browsing data.

- Tap **Default Browser** to select the default browser for you device.
- Tap **Clear Browsing Data** to delete your cache an other browsing data from the built-in browser.

Debug Information

Enables activity logging, lets you send the log file to an email address, and provides GCM and MDM diagnostic information.

Do not change the **Enable Debug Logging** setting–this value is set by your IT department.

Profile Management

Lets you unregister the device. See "Unregistering Your Device" on the next page for further detail.

Terms

Displays the terms of use.

Using App Lock

This icon locks the Delinea application. If you do not have a PIN configured, then you are prompted to create one. You can also use your fingerprint for authentication if your device supports fingerprinting.

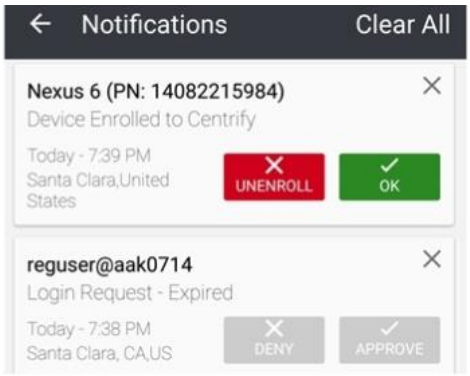
Configurations made by the system administrator override your user configuration.

See "Securing Your Delinea Application" on page 390 for configuration information.

Pending Notifications

Notifications to which you have not responded can be accessed via the bell icon. The number associated with the icon shows the number of pending notification.

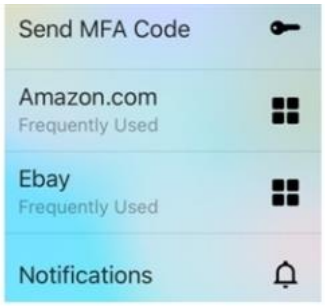
Tapping the icon displays the notifications. Expired notifications (such as MFA notifications where the default response time is 10 minutes) are grayed out and you cannot take action on them.



Accessing Shortcuts

You can access the following shortcuts by long-pressing the Privileged Access Service application icon:

- Multi-factor access (MFA) options
- Top two frequently used applications
- Pending notifications



Important: This feature is only supported on Android 7.1 and newer.

Unregistering Your Device

Unregistering your device from the Privileged Access Service removes the mobile device policies from your device. It does not, however, remove the Delinea application from your device. The next time you open the Delinea application, it prompts you to register the device.

- The ability to unregister your device is controlled by your IT administrator. This option may not be available to you.

> **Note:** If you are upgrading the Delinea application from a previous version, remove any version that is version number 13.8 or earlier. The Settings screen in the Delinea application shows the version number.

The following procedure unregisters the device. If you want to uninstall the Delinea application as well, use the standard Android Application manager procedure.

To unregister an Android device:

1. Open the Delinea application on the device.
2. Tap **Settings**.
3. Scroll down and tap **Unregister**.

   If you do not see the Unregister option, it means that you do not have the permission to unregister this device.
4. Confirm that you want to remove your profiles.

Uninstalling the Delinea Application

Before you can uninstall the Delinea application from an Android device, you must first unregister the device from the Privileged Access Service – see "Unregistering Your Device" on the previous page.

After you have unregistered the device, you use the Android device's application manager to remove the Delinea application.

Registering an iOS Device and Using the Delinea Application

You register your device in the Privileged Access Service using the Delinea application. If you have not installed the Delinea application, see "Using Devices" on page 383 then return here to complete device registration.

Your organization may also configure mobile device policy profiles. The profiles set system preferences that configure communications with your corporate network and may impose some restrictions on your use of some device features.

The following topics are relevant to registering a device and using the Delinea application:

Registering an iOS Device

You use the Delinea application to register the device in the Privileged Access Service. After you register the device, you use the Delinea application to open the web applications that were assigned to you by your IT department.

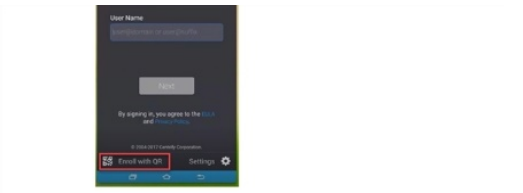
To register your device:

1. Open the Delinea application on your device.
2. Enter your user name and password.

   Your IT administrator will provide you with the user name and password you should use.
3. (Contingent upon configuration) If your systems administrator has enabled the feature, you can register your device without entering your user name and password. Do the following:

a. Tap **Register with QR**.

The scanning tool opens.



b. Scan the QR code on **Admin Portal > Profile > Devices > Add Devices**.

c. Click **Proceed** on the device browser.

4. Tap **Allow** if you want the Privileged Access Service to show your device's location on the Admin Portal.

The Delinea application opens to a screen that lists the web applications that have been deployed to you by your Privileged Access Service administrator. See "Using the Delinea application" below.

Using the Delinea application

You use the Delinea application to view and manage system resources from your device. Also, if your IT department requires a one time passcode to log in to the Admin Portal, you use the Delinea application to generate the one-time passcode.

Securing your Delinea application

You can secure your Delinea application using a PIN or biometrics. After you configure these security settings and enable the application lock feature, you will be prompted to use one of the configured methods (PIN or biometrics) to access the Delinea application.

To secure your Delinea application:

1. Tap the Delinea application on your device.
2. Tap **Settings > Security Settings**.
3. Enter a PIN as your primary access method.
4. (optional) Register your biometrics as an alternative access method.

If biometrics recognition is available on your device, then we direct you to the device biometrics registration window.

5. Tap the **App Lock Settings** option on the Settings page and enable the feature using the **Lock on Exit** field.

The setting defined by your system administrator overrides your settings here.

6. (optional) Tap **Auto-Lock** and configure how long you want the Delinea application to be inactive before it automatically logs you out.

You will now be prompted to use one of the configured methods (PIN or biometrics) to access the Delinea application.

Changing Your Active Directory or Delinea Application Password

If you have a Privileged Access Service User account, changing your password changes the password you use to open the Delinea application and to register devices. If you have an Active Directory User account, this also changes the password you use to log in to your company account when you start up your computer.

Your IT administrator controls whether or not you can change your password.

If you have an Active Directory User account, you may need to change other passwords as well. For example, if you log in to Outlook with the same account, you'll need to change that login password to match. Confirm with your IT staff regarding other passwords you may need to change after you change your Active Directory User account password in the Delinea application.

To change your account password on your device:

1. Tap the Delinea application on your device.
2. Tap **Settings > Change Password**.
3. Enter your current and new passwords.
4. Tap **Save**.

Checking Out an Account Password

Delinea lets you securely store user name and password combinations in the Privileged Access Service for local accounts. You can use those accounts to log on securely to the servers, switches, and routers you identify as *Systems, Domains, and Databases*.

In addition, you can check out passwords for Delinea-managed local administrator accounts for registered devices. You can either show the password or copy it to the clipboard, then use it to perform operations that require admin rights.

Checking out an account password requires the following:

- Appropriate administrative rights on the Delinea identity platform.
- Existing access to Delinea privilege service (for Systems accounts).
- The device must be registered in the Privileged Access Service.
- Your authentication mechanisms must be configured for the Delinea application–see "Securing your Delinea application" on the previous page.

Account Types You Can Check Out

The following are account types you can check out passwords for:

- Tap **Systems** on the Delinea application to see available systems and check out the password for a stored account.
- Tap **Domains** on the Delinea application to see available domains and check out the password for a stored domain.
- Tap **Databases** on the Delinea application to see available domains and check out the password for domains.

> **Note:** You need view and checkout permission to check out a system, domain, or database password.

When you check out a password, it remains checked out until either you check it back in or the checkout time expires. The maximum check out time is configured by your admin through policy; however, you can extend the checkout time for a password that is currently checked out. When you extend the time, it is reset to the maximum check out time.

Checking Out a Password

For detailed steps on how to check out a password, see "Checking Out an Account Password" on the previous page. You can view these operations in the activity stream of the resource in portal. To do this: navigate to a resource, select the resource and choose the **Activity** tab.

Using Privileged Access Service as an Authenticator

You can use the Privileged Access Service Admin Portal to get the one time passcode (either by scanning an external source's QR code or entering the authentication key information manually). You then can use the passcode to log in to the relevant application or website.

To Scan a QR Code

To scan a QR code, you must use the Privileged Access Service Admin Portal application on an registered mobile device.

1. Log in to the Privileged Access Service application on your mobile device.
2. Tap **Passcodes**.

   The Authentication window shows any existing passcodes.
3. Tap the plus icon (**+**) then tap **Scan QR Code**.
4. Scan the external source's QR code.

   The Passcodes window shows the newly generated passcode. The newly added authentication account is also added to the Passcodes page in the Accounts section of the Admin Portal.

To enter the authentication key information manually on your mobile device

To enter the authentication key information manually, you can use the Privileged Access Service Admin Portal on your mobile device or computer. See "Managing Authentication Keys" on page 388 for information on entering the authentication key information manually using your computer.

1. Log in to the Privileged Access Service application on your mobile device.
2. Tap **Passcodes**.

   The Passcodes window shows any existing passcodes.
3. Tap the plus icon (**+**) then tap **Enter Authentication Key**.
4. Enter the information provided by the application or website.
5. Tap **Save**.

   The Passcodes window shows the newly generated passcode. The newly added authentication account is also added to the Passcodes page in the Accounts section of the Admin Portal.

Using App Lock

This icon locks the Delinea application. If you do not have a PIN configured, then you are prompted to create one. You can also use your fingerprint for authentication if your device supports fingerprinting.

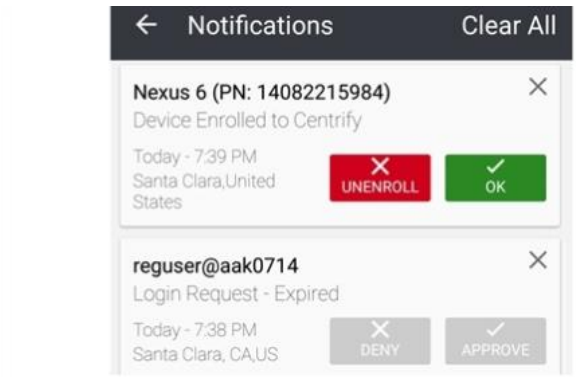
Configurations made by the system administrator override your user configuration.

See "Securing your Delinea application" on page 396 for configuration information.

Pending Notifications

Notifications to which you have not responded can be accessed via the bell icon. The number associated with the icon shows the number of pending notification.

Tapping the icon displays the notifications. Expired notifications (such as MFA notifications where the default response time is 10 minutes) are grayed out and you cannot take action on them.



Using the Settings Screen

The Settings screen contains device configuration information such as default browser settings, authentication settings, and other useful information.

Debug Options

Allows you to enable/disable the debug mode for the Browser Extension. You will typically use this setting while working with your system administrator.

Browser Settings

You use this option to set your default browser and clear browsing data.

- Tap **Default Browser** to select the default browser for you device.
- Tap **Clear Browsing Data** to delete your cache an other browsing data from the built-in browser.

Log Settings

Allows you to configure log file related information. Options are:

- Log Level

  Sets the level at which log files are logged.

- Log to Console

  Sets the level at which log files are sent to the console.

- Send Log File

  Provide the email addresses to which the log files should be sent.

Privileged Access Service Settings

The URL option contains the Privileged Access Service service URL.

Do not change this setting unless specifically instructed to by your IT department. If the URL is wrong, you cannot use the Privileged Access Service.

Apps Settings

Lets you show/hide applications that are not supported on mobile device browsers.

When you tap an application that cannot be run, the Delinea application displays an error message and gives you the option to hide it and all other applications that are not supported. Tap **Hide All** to remove these applications from the screen.

To display the hidden applications, open the **Settings** tab in the Delinea application and configure the **Show All Applications** option.

Authentication

Lets you configure the following:

- Mobile authenticator -- See "Using Multi-Factor Authentication" on page 363.
- Change Password -- Allows you to change your Active Directory or Privileged Access Service account password. See "Changing Your Network Login Password" on page 388.

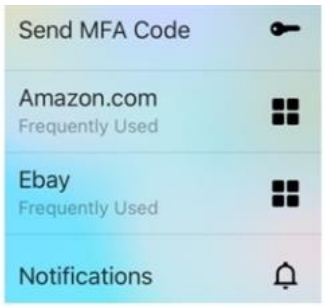
Terms

Displays the terms of service and use, privacy policy, and acknowledgments.

Accessing Shortcuts

You can access the following shortcuts by long-pressing the Privileged Access Service application icon:

- Multi-factor access (MFA) options
- Top two frequently used applications
- Pending notifications



Important: This feature is only supported on iOS 7 and newer.

Unregistering an iOS Device

You unregister a device to remove the Privileged Access Service profiles from the device's settings. You can register the device again using the Delinea application.

Note: The ability to unregister your device is controlled by your IT administrator. This option may not be available to you. If your device is assigned to the Apple Device Enrollment Program, you cannot unregister it.

Unregistering removes the profiles installed when you registered the device.

To unregister an iOS device:

1. Tap the Delinea application icon on your home screen.
2. Tap **Settings**.
3. Scroll down and tap the **Unregister Mobile Device** button at the bottom of the screen.

   If you do not see the Unregister Mobile Device option, it means your IT department has not given you the permission to unregister.
4. Tap **OK** to confirm that you want to unregister.

   After unregistering is complete, the Delinea application displays its log in screen.

Registering a Device

Privileged Access Service requires the device owners to register the device regardless of whether it is used for single sign-on or mobile device management.

Before users can register a device, ensure that the relevant pre-requisites have been met. See "Device Registration Prerequisites" on the next page. Additionally, the relevant user accounts must have the register device permission. See "How to Register Devices" on page 404 for the details.

Users register their devices using the following methods, depending on device OS:

- **Android devices:** Users "Installing the Delinea Mobile Application" on page 383 for Android on the device.
- **iOS devices:** Users "Installing the Delinea Mobile Application" on page 383 for iOS on the device.

Device Registration Prerequisites

Before you start configuring user accounts for device registration, make sure you have met the relevant IP address, port, and hostname requirements.

Privileged Access Service Connection Requirements

All connections to the internet made by Privileged Access Service (including Delinea Connector and mobile management) are outbound in nature. No internet facing ingress ports are required. All outbound connections are made via TCP to either port 80 or 443 and should not have any restrictions.

To provide the redundancy and availability of an always available Privileged Access Service, the destination resource, IP address, and host for outbound connections will vary over time amongst thousands of addresses. Additionally, the range of which also changes as new resources are provisioned or removed.

Note: Use of deep packet inspection filtering of HTTPS or SSL traffic by web proxies or security software may cause connectivity issues with Privileged Access Service. In all cases, the ports and addresses discussed below should be excluded from packet inspection to allow for normal service operation.

Option 1: Whitelist Source

Given the variability of connection targets, the simplest whitelist configuration is typically one where filters are based on the traffic source. Specifically, it relates to configurations where you allow all outbound traffic from the host machine and account running the Delinea Connector and for outbound requests made by iOS, Android, and Mac clients. This whitelist may be scoped at the machine, or machine + account, or machine + account + process level depending on the feature set of the security appliance or process in place.

Option 2: Whitelist Source Ports

You can also use a whitelist configuration where all outbound traffic on ports 80 and 443 is allowed from the host machine and account running the Delinea Connector, as well as outbound requests made by iOS, Android, and Mac clients. This whitelist may be scoped at the machine, or machine + account, or machine + account + process level depending on the feature set of the security appliance or process in place.

Option 3: Whitelist Destination

If destination whitelisting is required, you can whitelist outbound ports or TCP Relay IP ranges.

Port numbers	Resource
443	`\*..centrify.com` or `\*.my.centrify.net` (if you need to whitelist your tenant URL)
80	www.public-trust.com
80	privacy-policy.truste.com
80	ocsp.digicert.com

If whitelisting an entire domain (`\*.centrify.com`) is not acceptable per security policy, then you need to whitelist the TCP Relay IP ranges for your relevant Privileged Access Service tenant region. Refer to https://www.microsoft.com/en-us/download/confirmation.aspx?id=56519 for a list of Microsoft Azure datacenter IP ranges by region.

AWS Tenants

If your tenant is on Amazon Web Services (AWS) servers, then you need to whitelist the IP ranges for your relevant Privileged Access Service tenant region. Download the relevant file that contains the IP address ranges information from https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html.

Use the table below to find the AWS TCPRelay IP address ranges for each tenant's region:

Region	IP Address Range
US East	3.14.30.0/27 (adding 4 May 2019) 13.58.135.200/29 18.216.13.0/26 34.236.32.192/26 34.236.241.0/29
US West	13.56.112.160/29 13.56.112.192/26 34.215.186.192/26 34.214.243.200/29
Canada	35.183.13.0/26 35.182.14.200/29
Europe	18.194.95.128/26 18.194.95.32/29 34.245.82.128/26 34.245.82.72/29
Brazil	18.231.105.192/26 18.231.194.0/29
Australia	13.211.166.128/26 13.211.12.240/29
Japan	13.231.6.128/26 13.231.6.96/26
Singapore	13.250.186.64/26 13.250.186.24/29

Region	IP Address Range
London	3.10.127.0/27 3.10.127.64/26 35.176.92.128/26 35.176.92.72/29

For additional information about whitelisting a tenant for use with web proxies and firewalls, see KB-13446.

Apple Device Specific Requirements

To register iOS or Mac devices, you must also allow traffic from Apple servers (.apple.com) iTunes servers (.itunes.com), and Apple Push Notification Service (APNS) servers. See https://support.apple.com/en-us/HT203609 for APNS port specific information.

Windows Device Specific Requirements

To register Windows devices, you must also allow traffic from Microsoft servers. Download the relevant file that contains the DNS and ports information from https://www.microsoft.com/en-us/download/details.aspx?id=44238.

Google Device Specific Requirements

To enroll Google devices, you must also allow traffic from Google servers. Download the relevant file that contains the DNS and ports information from https://firebase.google.com/docs/cloud-messaging/concept-options#ports_and_your_firewall.

How to Register Devices

This scenario is intended to guide system administrators through the procedures for enabling users to register devices. Users typically register their own devices, but system administrators must enable the relevant settings. When devices are registered, you can manage them in Admin Portal, install mobile device policies, and deploy mobile applications to specified devices.

Registering a device requires Privileged Access Service to push a user certificate to the device. Typically, we use the User Principle Name (UPN) as the subject alternative name of the certificate. If you want to use Distinguished Name (DN), please contact Privileged Access Service Support.

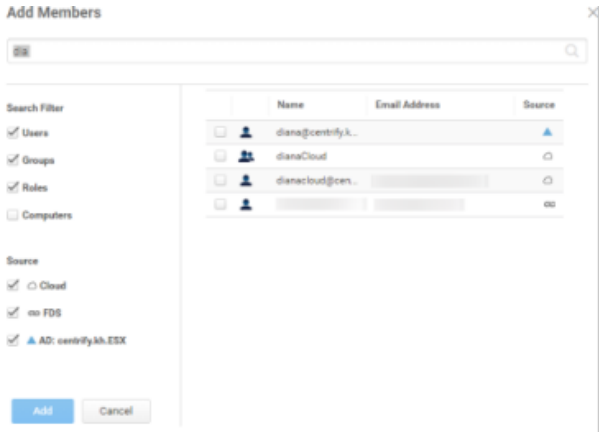
Note: If you have the Direct Control agent installed, you must remove it before installing the Delinea Mac Agent version 19.5 or higher to use MFA for Mac. The MFA for Mac feature is not compatible with the Direct Control agent. Refer to Installing and removing the agent and leaving a domain for more information about uninstalling the Direct Control agent and leaving an AD domain.

This scenario includes the following topics:

Enable Users To Register Devices

Before a user can register a device, you must provide this user with the relevant policy set.

1. Log in to Admin Portal.
2. Click **Access > Roles**.
3. Create a new role or select an existing role.
4. Click **Members > Add**.
5. On the Add Members window:
   a. Enter the first few letters of the user, role, or Active Directory/LDAP account/group you want to add and click the search icon.
   b. Select the relevant user, role, or Active Directory/LDAP account/group and click **Add**.



6. Click **Save** to save the changes.
7. Click **Policies** and either click **Add Policy Set** or select an existing policy.
8. Click **Devices > Device Registration Settings**.
9. Select **Yes** in the **Permit device registration** policy.
10. Configure the remainder of the policy settings.

    These settings apply regardless of whether you use the Delinea directory policy service or Active Directory group policies to manage device configuration policies:

Device registration control settings	To enforce these limitations
Allow user notifications on multiple devices	Select **Yes** to send authentication notifications to multiple registered devices and **No** to send to the first registered device only (default setting), or "--" to use the default setting.

Device registration control settings	To enforce these limitations
Enable debug logging	There are two logging modes on devices: regular - the default setting - and debug logging. Use this policy to turn on the debug logging mode. Select **Yes** to enable debug logging, **No** to set regular logging, or "--" (Not configured) to use the default setting.
Enforce fingerprint scan for Mobile Authenticator	Select **Yes** to require that users provide a finger print scan to use mobile authenticator. Using the associated policy option, users can alternatively use the client application PIN for access. The default setting is **No**.
Permit non-compliant devices to enroll	Prevent noncompliant devices from enrolling. To enable users to enroll a noncompliant device, select **Yes** in the drop-down menu. Open the tool tip for more information on this policy.
Report mobile device location	Select **Yes** to allow devices to report their location, **No** to stop the device from reporting location, or "--" to use the default setting (Yes).
Require client application passcode on device	Select **Yes** to require a passcode to open the client application, **No** to allow opening the client application without a passcode, or "--" (**Not configured**) to use the default setting. **Note**: You must select **Yes** to enable other client application passcode policies.

11. Click **Save**.
12. Click **Policy Settings**.
13. Specify the policy assignment:
    - **All users and devices:** Applies this policy to all users and devices registered on Privileged Access Service.
    - **Specified Roles:** Click **Add** to select the roles to which you want this policy applied.
    - **Sets (NOT applicable for unregistered devices):** Specify the set type (currently only Device type is supported) for registered devices and the set parameters (iOS devices, corporate owned devices, and so on). Sets are a collection of devices, users, etc.

      Important: Do not use this option when configuring a policy for device registration. Sets only apply to registered devices. If you assign this policy to users who do not already have a device registration policy (through the All Users and Devices or Specified Roles option), device registration will fail.
14. Click **Save**.

What Happens When a Device is Enrolled

When the user enrolls a device, Privileged Access Service performs the following actions:

- The device is added to the Profile page in Admin Portal.

  If the user has an Active Directory account, the device is also added to the Active Directory organizational unit specified in the Device Enrollment Settings.

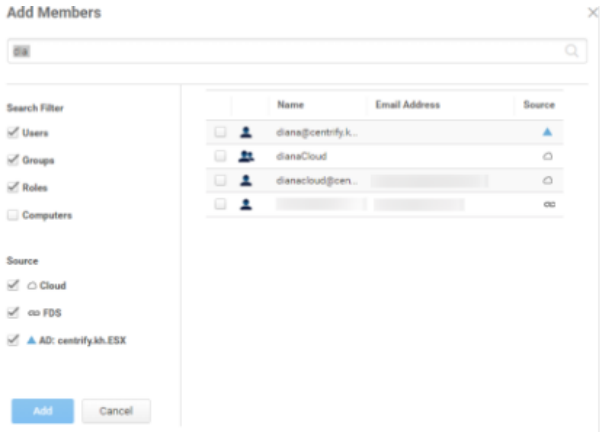
Enabling Invitation-Based Device Enrollment

This option allows users to enroll their devices without entering their system password. Users select the link and certificate exchanges happen automatically. This option is ideal for smart card users to enroll their mobile devices because these users do not have passwords.

Both Android and iOS devices are supported.

To enable invitation-based enrollment mobile devices:

1. Log in to Admin Portal.
2. Click **Access > Roles**.
3. Create a new role or select an existing role.
4. Click **Members > Add**.
5. On the Add Members window:
   a. Enter the first few letters of the user, role, or Active Directory/LDAP account/group you want to add and click the search icon.
   b. Select the relevant user, role, or Active Directory/LDAP account/group and click **Add**.



6. Click **Save** to save the changes.
7. Click **Policies** and either click **Add Policy Set** or select an existing policy.
8. Click **Policies > Devices**.
9. Select **Yes** in the **Enable invite based enrollment** policy.
10. Select the length of time (in minutes) that the invitation will remain valid in the **Invite based enrollment link expiration (default 60 minutes)** policy.
11. Configure the other policies as necessary.
12. Click **Save**.

Re-Registering a Device in Domains With a Different Customer ID

If your organization has multiple customer IDs in the same forest, you might encounter a situation in which users cannot unregister a device from one domain and then register it in another. When they try to register it in the new domain, they get the message:

```
A transaction with the server at \<server name\> has
failed with the status “403”.
```

This situation can occur when you have multiple connectors, each with a different customer ID, and each connector uses a different Active Directory container to store the device object. There are a couple of common situations in which this can occur:

- When you have a test and production deployments each in a separate domain and each domain has a separate Privileged Access Service customer ID.
- When your organization has different divisions—for example, a North America and APAC division—with separate domains and Privileged Access Service customer IDs.

The administrative problem is this: the same device cannot have separate objects in two different organizational units within the same forest. This is a problem because unregistering a device does not delete it from the organizational unit. When the user unregisters a device, the Privileged Access Service just changes the state from registered to unregistered.

To allow the user to register the same device in another domain with a separate customer ID an administrator needs to do one of the following:

- Grant the destination connector permission to move or remove objects (in this case, the device object) in the original connector’s organizational unit.
- Manually delete the device object from the original connector organizational unit when the user unregisters the device. You can do this in ActiveDirectory or using Admin Portal. When the user registers the device the nexttime, the Privileged Access Service creates a new object in the destination organizational unit when the user registers the device.
- Manually move the device object from the original connector organizational unit to the destination after the user unregisters it. When the userregisters the device the next time, the Privileged Access Service updates the state to registered device in the destination organizational unit.

Configuring the Connector

The Delinea Connector enables secure communication between your internal network (AD or LDAP) and Privileged Access Service.

You can use the Delinea Connector to authenticate Privileged Access Service users by using their Active Directory or LDAP account or if you are adding resources and shared accounts to Privileged Access Service. Additionally, you can install additional connectors for load balancing and failover.

The Delinea Connector runs on a server that is joined to your domain (best practice is to not install on the domain controller) and manages communications between Active Directory/LDAP and Privileged Access Service. It also monitors Active Directory for group policy changes, which it sends to Privileged Access Service to update registered devices.

To integrate your Active Directory/LDAP service with Privileged Access Service, you need to install at least one connector on your network inside the firewall.

You can also install a Delinea Connector outside of Active Directory for use with gateway-based auditing. For details, see "Enabling Auditing for Remote Sessions" on page 805.

Updating HSTS header

The HSTS header enables you to use strict transport security on the connector service. The HSTS header is added by default to the Connector IWA Web Server response.

To turn the header on / off, use the registry setting on connector machine:

1. The registry path is: `HKEY_LOCAL_MACHINE\SOFTWARE\Centrify\Cloud\`.
2. If the registry keys do not exist, create them using DWORD (32-bit) values.
3. Set EnableHSTS to `0` (OFF) or `1` (ON).
4. Set the age of the User registry with the setting HstsAge. The default value is `31536000`.

Determining Whether You Need a Connector

The Delinea connector is a multipurpose service that provides support for key features and enables secure communication between other services on your internal network or a cloud instance. Not all services require a connector, however. For example, if all users are Privileged Access Service user accounts, the connector isn't required.

You must have at least one connector if any of the following apply:

- You are using Active Directory or another LDAP server as the identity store.
- You manage access to applications through an application gateway.
- You are using Privileged Access Services for privilege elevation, privileged account request and approval work flow, or shared password management.

You can install more than one connector to support fail-over and load balancing. If you need to use a connector, you can download the software package from within the Admin Portal or from the Infrastructure step in the Quickstart wizard. For more information, see ""How to Install a Connector" below.

How to Install a Connector

The Delinea Connector is a multipurpose software that enables secure communication between your internal network and Privileged Access Service.

You install the Delinea Connector for the following purposes:

- If you are authenticating Delinea Directory users by using their Active Directory or LDAP account or if you are adding resources and shared accounts to Privileged Access Service.
- Install additional Delinea Connectors for load balancing and failover.
- To integrate your Active Directory/LDAP service with Privileged Access Service, you need to install at least one connector on your network inside of the firewall.

You can install more than one connector for your organization to support fail-over and load balancing. You might also want to install more than one connector if you are using multiple Privileged Access Service services. In most cases, you should install two connectors in a production environment. Delinea determines which connector to use by monitoring connector health and making a random selection with a bias toward healthy connectors.

Industry best practice recommends that you do not install the connector on the same server as the domain controller. Domain controllers are single-purpose systems.

Delinea recommends "How to Auto-update Connector Software" on page 421 to keep up-to-date with the current version of the connector; however, we understand that in some environments it might not be possible to update software that has gone into production environments. Therefore, Delinea connector installations are supported up to the last two previous versions.

Overall Requirements

To install and configure Delinea Connector you need the following:

Item	Description
Privileged Access Service Management Suite installer	This program installs the connector, Active Directory/LDAP and group policy console extensions, and the Delinea Connector Configuration Program. To get the installer, you open Admin Portal, click **Settings**, **Network**, **Delinea Connectors**, and **Add connector**. Repeat this procedure every time you install a connector to ensure you get the latest version of the connector.

Item	Description
Host computer joined to the domain controller	You install the Centrify Connector on a Windows computer to establish the communications link between the Privileged Access Service and Active Directory domain controller. If you are referencing accounts in an Active Directory tree or forest, the connector can be joined to any domain controller in the tree (it does not need to be the root). In addition, that domain controller must have two-way, transitive trust relationships with the other domain controllers. See "Supporting User Authentication for Multiple Domains" on page 448 for details. This computer must be in your internal network and meet or exceed the following requirements: - For the latest version of supported Windows Servers, see the Centrify PAS release notes at "PAS and Cloud Suite Release Notes" on page 1199. All running 64-bit with 8 GB of memory, of which 4 GB should be available for connector cache functions. - Has Internet access so that it can access the Privileged Access Service. - Has a DigiCert Global Root CA certificate installed in the Local Machine Trusted Certificate root authorities store. - Microsoft .NET version 4.8 or later; if it isn't already installed, the installer installs it for you. - Be a server or server-like computer that is always running and accessible.
Permissions on the connector machine	To install the Delinea Connector, you need to be the local administrator on the Delinea Connector machine. See "Installation and Service Account Privilege Requirements" below for more permissions requirements.
Firewall and external IP address requirements	See "Firewall and External IP Address Requirements" on page 453
Execute VBScript	The server must be able to execute VBScript during the installation.
Web proxy server (optional)	

Installation and Service Account Privilege Requirements

Installing the connector requires file installation (running the installer.exe file) and registration (running ProxyUI.exe for the first time). File installation requires local administrative permissions on the connector machine because you need to copy files to Program Files, set up Windows service, modify registry, etc. Registration also requires local

administrative permissions because you need to write the settings to registry. However, additional permissions may be required depending on what you want to do.

Services	Required Rights and Privileges
Synchronize deleted objects in Active Directory with Privileged Access Service	When you delete users in Active Directory and want this deletion synchronized with Privileged Access Service, you have two options: - You must be the domain administrator of the Active Directory domain for the relevant deleted objects container. If you are deleting users in multiple domains, make sure that you are the domain administrator for all those domains. - Delegate read permissions to the service account for the deleted objects container in the corresponding domain. If you do not take one of the above actions, users deleted in Active Directory will be listed on the Users page in Admin Portal until you manually delete them. However, they will not have access to any Privileged Access Service functionalities. See "How to Delete User Accounts" on page 233 for more information on deleting Active Directory accounts.
Register the connector as an Active Directory proxy (for example, only for App Gateway)	If you want to register a connector as an Active Directory proxy, you need to have Read permissions to the Active Directory server.
Register the connector in your Privileged Access Service account	

All Active Directory accounts are members of the built-in Authenticated Users group. By default, members of the Authenticated Users group have list and read permissions on most Active Directory objects. The specific permissions vary for different object types and Active Directory versions.

You can also install the Delinea Connector on non-Active Directory computers. In this case, you can use local (i.e. non-Active Directory) accounts.

Permissions Required for Alternate Accounts and Organizational Units

You can run the connector service as an Active Directory service account instead of as a Local System account. The account you select must have all of the required permissions. For example, if you run as a specific Active Directory service account, the account must be a member of the local administrators group, and you must confirm that it has at least read permission to the container that has Privileged Access Service user accounts and Active Directory Groups used as members of Roles.

You should not run a Windows service with an Active Directory built-in account or an Active Directory user account.

You must verify that the relevant accounts have permission to read Active Directory users and groups as if authentication would work. Each time role permissions are reassessed, the Connector tries to resolve the Active Directory groups mapped to any role in which the Active Directory user is potentially a member.

The host computer must also have read access to the container or organizational unit (OU) that stores the user accounts. Without read access, the connector cannot authenticate the user. Domain computers have this permission by default; however, the connector host may not. This most often occurs in multi-forest or multi-domain setups and can occur even when two-way trust is already defined. You can tell when this occurs—the connector log would show the error message, "unable to locate forest or user object."

In this case, you need to give the Local System account read access permission to the containers or organizational units.

To set the Read access permission to the user account container or organizational unit:

1. Open Active Directory Users and Computers, select the user account container, and open the **Properties**.
2. Select the **Security** tab and then click **Add** to add the user account you are using to run the connector service. Click **OK** after you add the user account.
3. Click the user account in **Group or User Names** and click the Allow box for the **Read** permission.
4. Click **OK**.

Any user or group that has been given permission to read and write the LockoutTime attribute for an OU or other container can unlock user accounts that reside in that container.

Password reset requires you to delegate a group of users to have the ability to reset passwords for another subset of users in a particular OU. See Password Reset Permissions for information on delegating password reset permissions.

Installing a Delinea Connector

Once you install the Centrify Connector you may integrate your Active Directory/LDAP service with Privileged Access Service. The connector allows you to, among other things, provide AD and LDAP based authentication to Privileged Access Service, RADIUS connectivity as well as RDP and SSH gateways to connect to systems.

Industry best practice recommends that you do not install the connector on the same server as the domain controller. Domain controllers are single-purpose systems. To install the connector, you must first get the Privileged Access Service Management Suite package then run the installation wizard.

Note: Before you install the Delinea Connector, you must ensure that your tenant URL is added to Internet Explorer's **Trusted sites** list.

Before You Begin

Before you install the connector, you must create a new role and assign that role the right to register and administer the connectors. To do this, do the following:

1. Create a new role: **Access** > **Roles** (add a role).
   a. Name the role Connector Administrator. The purpose of this role is to create and manage the addition of connectors to the system.

b. On the Administrative **Rights** tab, add the right to **Register and Administer Connectors** and click **Save**.

2. Navigate to **Access** > **Users** and create a new cloud user by clicking **Add User**. Name this user **connectoradmin**. Add the email address, display name, password, and click **Create User**.
3. Navigate back to **Access** > **Roles** and click the Connector Administrator role. Go to the **Member** tab and add the user **connectoradmin** to the Connector Administrator role and click **Add**.

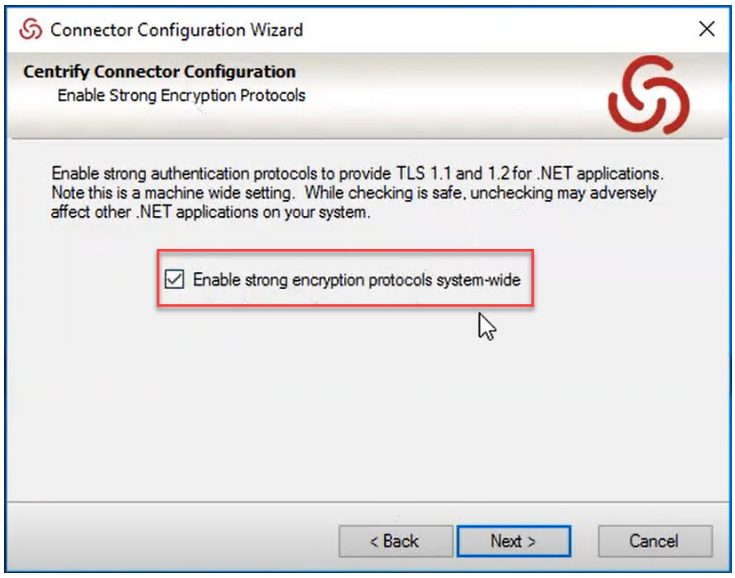
> **Note:** The above steps must be completed before you proceed to installing the connector.

Installing a Connector on a Host Computer

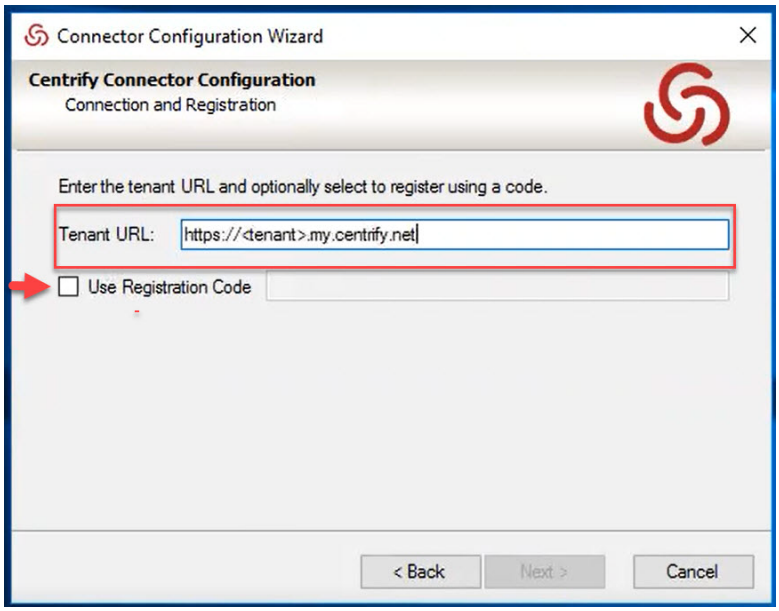
1. Download the Delinea Connector installer:
   a. Log in to the host computer with an account that has sufficient Delinea Connector permissions to install the connector.
   b. Open the Admin Portal.
   c. In the navigation pane, click **Downloads** and search for "Delinea Connector" or scroll down to see the connector file.
   d. Next to the Delinea Connector file, click **Download** to download a zip file.
   e. Extract the zip file and then run the installer program **Centrify-Connector-Installer-<version>.exe**.
2. Click **Yes** to continue if the User Account Control warning displays.
3. Click **Next** on the Welcome page. Review the End User Software License and Services Agreement, accept the terms of agreement, then click **Next**.
4. Select the components to install, then click **Next**.

> **Note:** The default is to install all components. Use the description on the installation UI determine what you want to install.

5. Click **Install** > **Finish** to open a second installation wizard. This second installation wizard initiates the connection between Active Directory and your Privileged Access Service tenant.
6. Click **Next** on the Welcome page.
7. You will next see the Delinea Connector Configuration wizard that allows you to set strong encryption protocols system-wide. The checkbox **Enable strong encryption protocols system-wide** is checked by default. Click **Next**.



8. Next, enter the **Tenant URL**:



and you can either:

- proceed to MFA, or
- you can choose to use a registration code. If you use a registration code, you bypass the MFA process. You do this by clicking the **Use Registration Code** checkbox. To obtain a registration code, you must obtain one from the Registration Codes utility in the Admin Portal as follows.

a. Navigate to the Admin Portal > **Settings** > **Network** > **Registration Codes**.

b. Here, you can add and manage connector registration codes.

For more information on managing connector registration codes, see "Using Connector Registration Codes" on page 418

9. If you have not used a registration code, you proceed to MFA and then step 13. If you used a registration code, you proceed with step 13.
10. Click **Next** unless you are using a web proxy server to connect to Privileged Access Service. If you are using a web proxy service, select the associated check box and specify the IP address, port, user name, and password to use.
11. Specify the monitored domains and relevant credentials to synchronize deleted objects in Active Directory/LDAP with Privileged Access Service, then click **Next**.

    When you delete users in Active Directory and want this deletion synchronized with Privileged Access Service, you have two options:

    - You must be the domain administrator of the Active Directory domain for the relevant deleted objects container. If you are deleting users in multiple domains, make sure that you are the domain administrator for all those domains.
    - Delegate read permissions to the service account for the deleted objects container in the corresponding domain.

    Note: If you do not take one of the above actions, users deleted in Active Directory will be listed on the Users page in Admin Portal until you manually delete them. However, they will not have access to any Privileged Access Service functionalities. The configuration wizard performs several tests to ensure connectivity.
12. Click **Finish** to complete the configuration and open the connector configuration panel, which displays the status of the connection and your customer ID.

    Note: If you are not authorized to retrieve a registration code, you will receive an error stating that.
13. Click **Delinea Connector** to view or change any of the default settings.
14. Click **Close**.

After you have installed and configured at least one connector, you can use either Admin Portal or your default browser to log on to Privileged Access Service. The next time you log on and see the welcome page, select **Don't show this to me again**, then click **Close**.

The column headings in Admin Portal associated with each connector indicate the following:

Column Header	Indicates
Delinea Connector	The name of the computer
Forest	The domain name for the domain controller to which the connector is joined.
Version	The version of the connector software. You can configure the connector to update automatically– see "How to Auto-update Connector Software" on page 421

Column Header	Indicates
Last ping	The last time the Privileged Access Service successfully pinged the connector.
Hostname	The DNS short name. You can also enter a fully qualified domain name to the IE local intranet zone. See "Enabling IWA Service on the Connector" on page 305 to change this name.
Enabled Services	AD Proxy -- Displays if the Active Directory proxy service is enabled on the connector. If enabled, it means you use the Active Directory proxy service to authenticate Privileged Access Service users who have Active Directory accounts. LDAP Proxy -- Displays if the LDAP proxy service is enabled on the connector. If enabled, it means you use the LDAP proxy service to authenticate Privileged Access Service users who have LDAP accounts. App Gateway -- Displays if the App Gateway service is enabled on the connector. The App Gateway service provides remote access and single sign on to web applications provided by internal web servers (see "Applications" on page 823 . RADIUS Client -- Displays if the connector is enabled for use as a RADIUS client. RADIUS Server -- Displays if the connector is enabled for use as a RADIUS server for customers who support RADIUS authentication. RDP Service -- Displays if the connector is enabled for remote desktop sessions using the remote desktop protocol (RDP) clients for access to target systems. SSH Service-- Displays if the connector is enabled for secure shell sessions using SSH clients for access to target systems. Web Server (IWA) -- Displays if the connector is configured to accept an Integrated Windows authentication (IWA) connection as sufficient authentication for users with Active Directory accounts. IWA is not available to Privileged Access Service account users.
Status	Active indicates that the Privileged Access Service can communicate with the connector. Inactive indicates that Privileged Access Service cannot communicate with the connector.

Installing a Connector from the Command Line

You can install a connector from a Windows or Windows PowerShell command line with the following command:

- `.\Cloud-Mgmt-Suite-version-win64.exe /quiet`

Where *version* refers to the version of the Connector that you download from the Admin Portal.

Configuring a Connector from the Command Line

After you have installed the connector, you can configure the connector from the command line, if desired.

To configure the connector from the command line:

1. Make sure that the connector is installed.
2. Run the Centrify.Cloud.ProxyRegisterCli.exe using one of the following formats:
   - Centrify.Cloud.ProxyRegisterCli.exe url=URL regcode=REGCODE
   - Centrify.Cloud.ProxyRegisterCli.exe url+RUL user=USERNAME pass=PASSWORD
   - Centrify.Cloud.ProxyRegisterCli.Exe url=URL bearer=BEARER

Where:
REGCODE is a valid connector registration code.
USERNAME and PASSWORD are the user name and password of an admin user.
This user must be able to login without MFA (Must be able to login with password only).
This user must have admin rights to register connectors.
BEARER is a valid user token.
URL is your tenant URL. For example, https://acme.my.centrify.net.

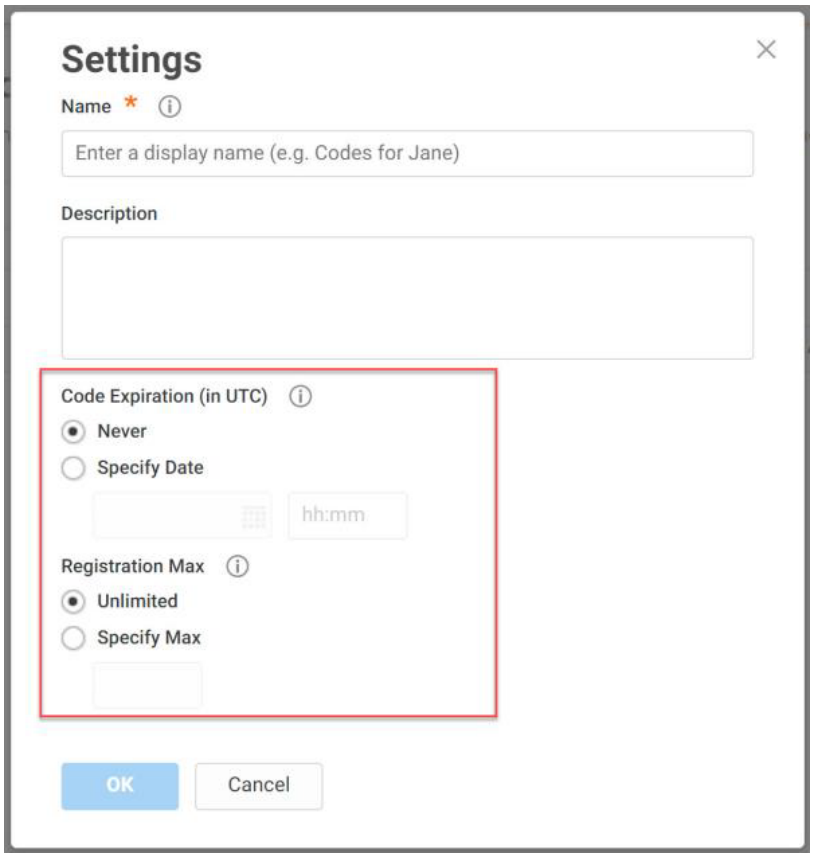
Using Connector Registration Codes

You can add and manage connector registration codes in the Admin Portal. You can add, modify, and delete connector registration codes. Additionally, you can easily download the Delinea Connector by clicking the download **Delinea Connector** link on the right-hand side of the page.

Note: You must be assigned the **Register** and **Administer Connectors** roles to access the connector registration codes functionality in the Admin Portal.

To add a connector registration code

In the Admin Portal, navigate to **Settings** > **Network** > **Registration Codes**. Click **Add**.Enter a name for the code. You can also set code expiration and registration max (maximum number of connectors that can be registered using that code) for the code(s) you are adding.



Once added, you can select an existing code, right-click and retrieve, modify, or delete a registration code.

How to Set the Service Connection Point (SCP) Object Permissions

The connector creates a serviceConnectionPoint object when it is started for the first time after installation. When the connector service is started by the Local System account, it has full control over the serviceConnectionPoint object.

If you use an Active Directory account other than the Local System account, the following procedure describes how to add the additional permissions required by that user.

Note: If you change the connector's account or modify Local System account permissions, be sure to make the same changes on all the connectors you install.

To set the permissions for a Service Connection Point (SCP) object for a selected user account:

1. Open ADSI Edit and open the **Properties** for the desired SCP object.

   The service connection is created when the connector is started for the first time. If the connector's name is

   CN=MachineA,CN=Computers,DC=domain,DC=com

   the SCP object is located in ADSI Edit at the following:

   CN=proxy,CN=MachineA,CN=Computers,DC=domain,DC=com

2. Select the **Security** tab and then click **Add** to add the user account you are using to run theconnector service. Click **OK** after you add the user account.
3. Click the user account in **Group or User Names** and click the **Advanced** button.
4. Click user account in the **Permission entries** tab and click the **Edit** button.
5. In the Object tab, click the Allow box for the **Write all properties** permission.

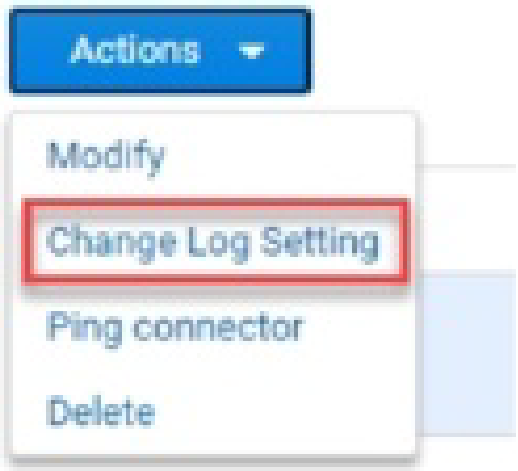
   The “Apply to” field should be set to **This object only**. This is often the default. If it is not, use the drop-down list to change it.
6. Click **OK**.
7. Click **OK** on the succeeding windows to exit ADSI Edit.

How to Change Connector Log Settings

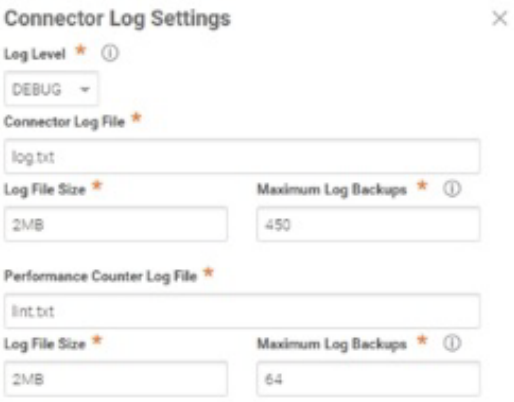
You can change the Delinea Connector log settings, such as the file size of logs collected on a connector host machine, the maximum number of backup files kept, and so forth.

To change the connector log settings

1. Log in to Admin Portal.
2. Click **Settings** > **Network** > **Centrify Connectors**.
3. Select the checkbox for the relevant connector.
4. Click **Actions** drop down list > **Change Log Setting**.



5. Make the necessary updates.



Note: Do not change the log file name unless instructed to do so by Delinea Support.

Log file size defaults at 2MB and max number of log backups defaults to 450 entries. Changing the file size will result in smaller log.txt files and modifying the log backup counter will limit the number of log.txt entries (log.txt, log.txt.1, log.txt.2, etc).

Logging Into the Administrator Portal with Silent Authentication

If you have Integrated Windows authentication enabled on the Delinea Connector (Integrated Windows authentication is enabled by default–see "How to Configure Integrated Windows Authentication" on page 304 for the details) and your browser is configured properly (see "How to Configure Browsers for Silent Authentication" on page 313 you can log in to Admin Portal without entering your Active Directory credentials. You simply add your login suffix to the Admin Portal URL in the following format:

`https://cloud.centrify.com/manage?customerID=<loginsuffix>`

For example, if your Active Directory login name is `bob.smith@bigcorp.com`, you would enter the following:

`https://cloud.centrify.com/manage?customerID=bigcorp.com`

`https://cloud.centrify.com/my?customerID=bigcorp.com`

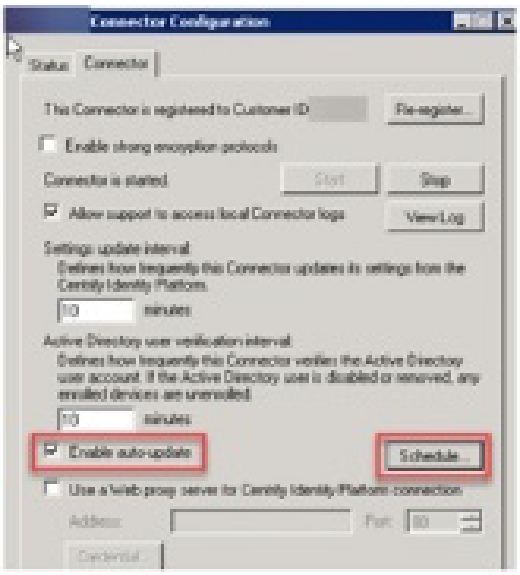
See "How to Use Login Suffixes" on page 236 to learn about login suffixes.

How to Auto-update Connector Software

You can configure the Delinea Connector to automatically poll Privileged Access Service for software updates and install them. The connector is enabled to poll automatically by default. You can also specify the auto-update time windows.

To configure software auto-update options:

1. Log in to the Delinea Connector server.
2. Open the Delinea Connector Configuration window.



3. Use the **Enable auto-update** check box to enable/disable the auto-update.
4. Use the **Schedule** button associated with the **Enable auto-update** option to configure the auto-update time window.
5. Click the **Apply** button.

To check for and install the connector

1. Click the Windows Start menu and open the Delinea Connector Configuration Program.
2. Click **Yes** to allows this program to make changes to the computer.
3. In the lower left of the Status tab, right-click the update icon and select **Update**.

   The connector updates and then displays a message indicating that the software is up to date.

How to Configure Frequency of Active Directory Updates

You can configure how frequently Active Directory updates (such as user account information, new domain controllers (DCs), etc.) are synchronized to Privileged Access Service. The default is 10 minutes.

To configure frequency of Active Directory updates

1. Log in to the Delinea Connector server.
2. Open the Delinea Connector Configuration window.

3. Use the **Settings update interval** configuration field to configure the frequency.
4. Click the **Apply** button.

Cloud Connector Guidelines and Best Practices

The Delinea connector provides a multipurpose service that supports key features and enables secure communication between other services on your internal network and a cloud instance.

Customers' different usages determine the deployment of connectors. For a long time, customers found it difficult to figure out how many connectors they need and the specifications of machines to install connectors on.

Note: The connector is an application that utilizes the CPU.

To better guide customers, we will show a comprehensive analysis of all features and product components utilizing the Delinea connector, and provide detailed assessments of the resource requirements for each.

Disclaimer

Many parameters impact connector performance, such as:

- Number of active users
- Number of concurrent users
- Types of features being used
- Applications being accessed
- Daily usage patterns

Note: An active user is someone who logs into the PAS at least once after their account is created. You can find all active users by going to **Access** > **Users** > **All Active Users**.

Even the way certain features are used can vary between companies, drastically impacting connector performance. For example, the types of commands used when accessing SSH or RDP services.

Given the wide range of customer use cases and usage patterns, it is impossible to provide an exact formula that fits all scenarios.

Once the system is up and running, it is important for customers to keep track of connector performance (CPU and memory) and adjust the connector settings accordingly.

Customer Categories

To classify customers for sizing purposes, we will use the following three tiers:

- Small (SMB): Up to 10k total users
- Medium (Mid Market): Up to 100k total users
- Large (Enterprise): Over 100k total users

The more total users a customer has, the more connector resources we will allocate to support their usage.

Connector Machine Configuration

You can install connectors on physical or virtual machines.

The machine requirements can be classified into the following sizes:

- Small: 2 Core 8 GB RAM, 500GB disk
- Medium: 4 Core, 16 GB RAM, 500GB disk
- Large: 6 Core, 32 GB RAM, 1 TB disk

> **Note:** All sizes should be served by 1 GB Ethernet.

Impact of Features and Capabilities

Using more features increases the load on the connector, so you may need additional connectors.

This is especially relevant for network and CPU intensive features, like:

- Session Monitoring (RDP or SSH)
- App Gateway
- Password Vaulting

It is recommended to designate **dedicated connectors** for supporting certain functionality, rather than using a single connector to serve any number of features together.

Connector Placement

For IWA-based login, the system selects a preferred connector based on the client's IP address and available connectors. Placement of the connectors relative to the user's Active Directory sites should be considered in relation to the user's Domain Controller.

The Radius Server functionality of the connector allows users to configure and distribute it according to the location and the load from the Radius clients, such as VPN servers.

Place SSH and RDP connectors close to the systems they are serving to improve connection and performance.

Guidelines

Light Traffic Use Cases

For light traffic use cases, such as IWA or simple authentication use cases, without heavy-load features like "session monitoring" or "application gateway", we recommend the following ratios:

- One small-sized connector per 4k concurrent authentications (only suitable for SMB customers)
- One medium-sized connector per 8k concurrent authentications (suitable for Mid-Market and some smaller Enterprise customers)
- One large-machine for every 10k concurrent authentications (suitable for Mid-Market and Enterprise customers)

See the below table for examples:

	Count
Total	7

Note: Each Active Directory forest should have its own set of connectors (based on the number of users it serves).

Provisioning Functionality

The connectors dealing with authentication can also typically handle the small amount of load that provisioning functionality adds to the connectors.

In medium environments (<100k users), you should add a dedicated set (2) of mid-sized connectors for provisioning.

In larger environments (>100k users) even more connectors should be added (recommend one connector for every 50k users).

Active Users	Number of Connectors (Medium Machines)	Number of Connectors (Large Machines)
20k	Not required	Not required
50k	1 + 1 (for redundancy)	1 + 1 (for redundancy)
100k	2 + 1 (for redundancy)	2 + 1 (for redundancy)
200k	Not recommended	4 + 1 (for redundancy)

App Gateway

App gateway performance highly depends on what users are doing, how much traffic/data users pass through, number of clients, and the number of connections.

We recommend designating **dedicated connectors** for app gateway support.

A single connector can support ~2k concurrent users for simple web applications (e.g. Jira, Jenkins).

Users may require additional connecters for more data intense applications (e.g. reporting).

Concurrent Users	Number of Connectors (Medium Machines)	Number of Connectors (Large Machines)
2k	1 + 1 (for redundancy)	Not required
4k	2 + 1 (for redundancy)	2 + 1 (for redundancy)
8k	4 + 1 (for redundancy)	3 + 1 (for redundancy)
16k	8 + 1 (for redundancy)	6 + 1 (for redundancy)

Note: As with other cases, redundancy should also be considered to ensure continuous availability.

SSH Session Monitoring

The SSH Session Monitoring functionality adds some load to the connectors. However, a large connector should be able to support hundreds of simultaneous connections.

We recommend designating dedicated connectors for SSH Session Monitoring.

We achieved a peak load of ~1,000 SSH sessions per connector under lab conditions, however, we would not recommend reaching this number.

A more reasonable guideline would be 1 medium-sized connector for 500 concurrent SSH sessions (750 SSH sessions for a large connector).

Note: SSH sessions vary in the amount of data they pass. We assume that our recommendations involve moderate traffic less than 1kb per second. Higher traffic rates (e.g. through automation) may require more connector resources.

Concurrent Sessions	Number of Connectors (Medium Machines)	Number of Connectors (Large Machines)
500	1 + 1 (for redundancy)	Not required
1k	2 + 1 (for redundancy)	2 + 1 (for redundancy)
2k	4 + 1 (for redundancy)	3 + 1 (for redundancy)
4k	8 + 1 (for redundancy)	6 + 1 (for redundancy)
8k	16 + 1 (for redundancy)	11 + 1 (for redundancy)

Note: As with other cases, redundancy should be considered to ensure continuous availability.

RDP (Windows) Session Monitoring

The RDP Session Monitoring functionality adds a substantial amount of load to the connectors.

We recommend designating dedicated connectors for RDP Session Monitoring.

We achieved a peak load of ~100 RDP sessions per large connector under lab conditions, however, we would not recommend reaching this number.

A more reasonable guideline would be 1 large-sized connector for 50 concurrent RDP sessions (using light traffic).

Concurrent Sessions	Number of Connectors (Medium Machines)	Number of Connectors (Large Machines)
50	Not recommended	1 + 1 (for redundancy)
100	3 + 1 (for redundancy)	2 + 1 (for redundancy)
500	15 + 1 (for redundancy)	10 + 1 (for redundancy)
1k	Not recommended	20 + 1 (for redundancy)

Note: As with other cases, redundancy should be considered to ensure continuous availability.

Discovery

Discovery heavily uses connector resources.

Note: We will update this section in the next few weeks once we gather additional measurements.

We recommend scheduling discovery for off-hours to ensure sufficient connector resources.

Other Features and Considerations

The connectors support many other features, which could impact performance and scalability.

For example: IWA, Radius Server, MFA, CDA (Direct Audit) Agent, and Discovery.

In general, we recommend dedicating connectors for such functionalities (not to mix with general authentication, provisioning, app gateway and session monitoring).

Note: We have not yet established sizing guidelines for these functionalities. We will assess the guidelines in the future, as needed.

Bulk updates to Active Directory may increase the load on connectors, so they should be scheduled for off-hours.

Users should consider Direct Audit (especially for RDP session recording) as it heavily consumes connector resources. More specific guidelines will be provided in the future.

How to Use Active Directory Certificates in Devices for Authentication

You can use a certificate authority in the Active Directory Certificate Service to generate user and computer certificates for user and device authentication. In turn, you can use these certificates for log-in authentication in the Wi-Fi, VPN, and Exchange ActiveSync server profiles rather than an account's user name and password.

Note: This section only applies when you use the Active Directory Certificate Service to issue your certificate. If you are using the Delinea Tenant Certificate Authority, you can skip this section. See

To use certificates from your Active Directory certification authority

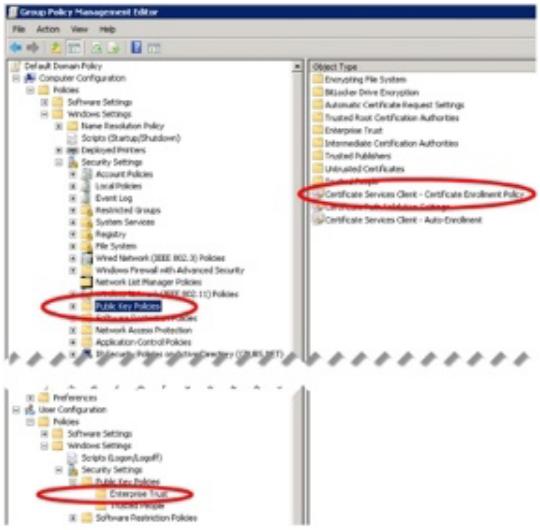
1. You must create user or computer certificate templates on the Windows Certificate Authority server used by the Delinea Connector. In addition, you need to configure the host computer for each of your Delinea Connectors so that it can revoke certificates. See "Creating the Certificate Templates" on the next page.
2. After you create the templates, the certificates are automatically created for and then installed by Privileged Access Service when the user registers the device.

- If you are using Active Directory group policy for device policy management, you can select the certification authority when you configure Device Policy Management–see "How to Select the Policy Service for Device Management" on page 738. If you are using Delinea directory policy service for device policy management and select the Active Directory Certificate Service, Privileged Access Service uses the default Active Directory Certificate Services certification authority only.
- In many cases, additional server configuration is required before you can use certificates for authentication. See your server's documentation for the details.

The procedures in this section assume that you have a working Active Directory Certificate Services certificate authority within your domain and you have sufficient permissions to modify the settings.

Enabling the Registration Policy to Use User and Computer Certificates

Before you can use certificates for authentication, you need to set the registration policy to enable automatic enrollment and renewal. The following procedure shows you how to set the Certificate Registration Policy for user and computer certificates in the Default Domain Policy. However, you can also set them on a group-by-group basis.



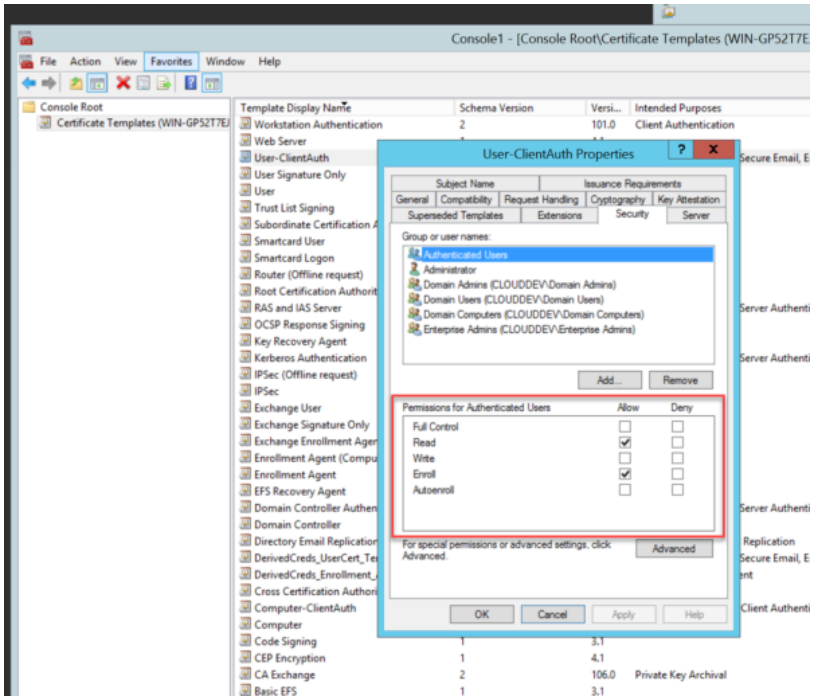
To enable computer and user certificate registration policies:

1. Open the Group Policy Management plug in on the connector, right-click the **Default Domain Policy,** and click **Edit**.
2. To enable the Certificate registration policy for computer certificates expand **Computer Configuration > Policies > Windows Settings > Security Settings** and click **Public Key Policies**.

3. Double click **Certificate Services Client - Certificate Registration Policy**.
4. In the **Configuration Model** menu, select **Enabled**.
5. Click **OK**.
6. To enable the Certificate registration policy for user certificates expand **User Configuration > Policies > Windows Settings > Security Settings** and click **Public Key Policies**.
7. Double click **Certificate Services Client - Certificate Registration Policy**.
8. In the **Configuration Model** menu, select **Enabled**.
9. Click **OK**.

Creating the Certificate Templates

The certificate templates you create can be used for configuring WiFi, VPN, and Exchange. The Certificate Authority server uses these templates to generate the client certificate that is installed on devices. When you configure WiFi, VPN, and Exchange to use a certificate template, you must ensure that the connector service account has Read and Register permissions. The following screenshot provides a reference. If you do not give these permissions, we cannot find the templates.



You create certificate user and computer templates on the Active Directory certificate authority server you defined. See "How to Select the Policy Service for Device Management" on page 738.

The templates you create must be named as follows, including the uppercase letters:

Computer-ClientAuth

User-ClientAuth

In some cases, you specify in the profile which type of certificate (user or computer) to use for authentication (for example, the iOS Wi-Fi profile) while others require you to use either the computer or the user certificate. To simplify profile configuration, we recommend creating both templates.

You use the Microsoft Management Console (MMC) on the certification authority server designated in the Delinea Connector to create the templates.

To create computer and user certificate templates:

1. Launch **certsrv.msc** or the Certificate Authority console on the Windows server with the certification authority installed.
2. Expand the certification authority, right-click **Certificate Templates**, and click **Manage**.
3. Right-click **Computer** choose **Duplicate Template**.

   To create the **User-ClientAuth** template, you right-click **User** instead and then choose **Duplicate Template**.
4. Click the **Compatibility** tab, select **Windows Server 2008** and click **OK**.
5. Click the **General** tab and enter **Computer-ClientAuth** in the **Template display name** text box.

   This action also automatically fills in the Template name field.

   If you are creating the user template, enter **User-ClientAuth** instead.
6. Set the Validity period: and Renewal period values.
7. Click the **Subject Name** tab and select **Supply in the request**.
8. Click the **Security** tab, select **Authenticated Users** and select the **Register** permission.
9. On the same tab, select **Domain Computers** and select the **Register** permission.
10. Click **OK** and close the Certificate Templates Console.
11. In the MMC, right-click **Certificate Templates**, click **New**, and click **Certificate Template to Issue**.
12. Click **Computer-ClientAuth** and click **OK**.

    If you are creating the user template, click **User-ClientAuth** instead and click **OK**.

    The templates you create should now appear in the Certificate Templates folder.

Revoking Certificates for Unregistered Devices

The certification authority does not by default revoke certificates for devices when they are unregistered. You must give the host computer for the Delinea Connector the "Issue and Manage Certificates" permission in the certification authority server to revoke certificates.

Note: You must grant this permission in the certification authority for the host computer for each of your Delinea Connectors.

To enable certification authority to revoke certificates when devices are unregistered:

1. Launch **certsrv.msc** or the Certificate Authority console on the Windows server with the certification authority installed.
2. Right-click the certification authority and click **Properties**.

3. Click the **Security** tab.
4. Click the **Add** button and select the host computer for the Delinea Connector.

   Make sure the “Computer” object type is selected (click **Object Types** and select Computers) and enter the first few characters of the computer name as the search filter in the Check Names field.

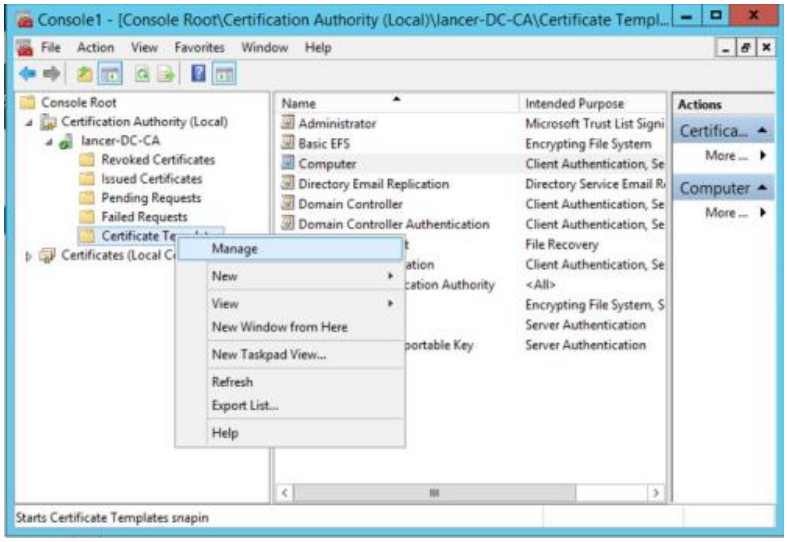
   Select the computer and click **OK**.
5. Select the computer from the Group or user names list and set the **Issue and Manager Certificates** permission to **Allow**.
6. Click **OK**.
7. Repeat this procedure for all of your connector host computers.

Creating a Connector Machine Certificate from an Internal Microsoft CA

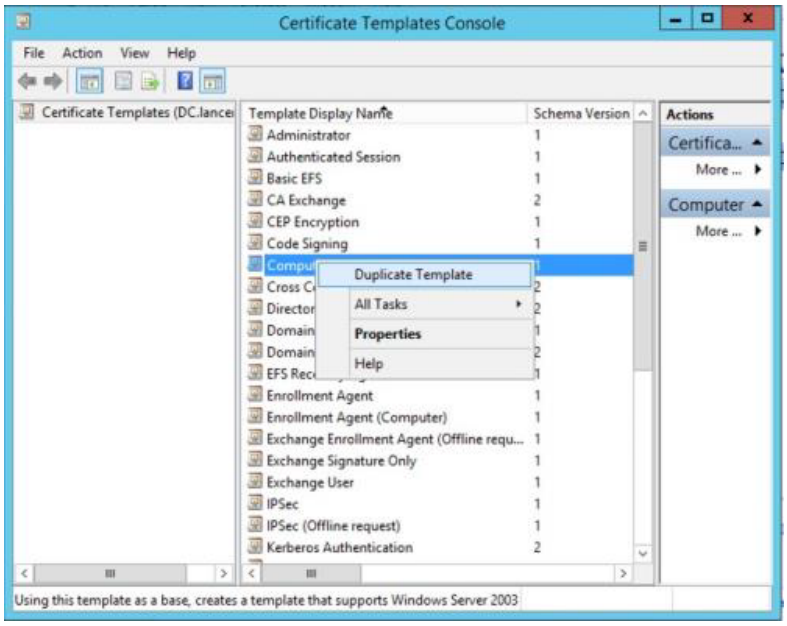
You can use the information in this section to guide you in creating a machine certificate for use with a connector in the Privileged Access Service. The connector requires a signed certificate and root of trust in order to communicate with the Delinea PAS.

To create a computer certificate template with an exportable private key

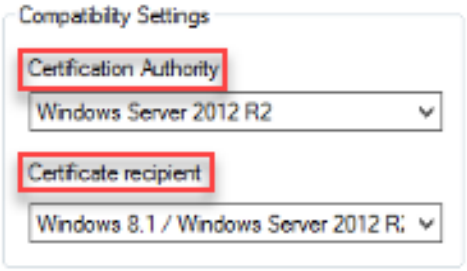
1. In your domain’s Certification Authority (CA), open the **Certification Authority** program and expand the CA.
2. Right-click **Certificate Templates** and select **Manage**.
   This opens the **Certificate Templates** console.



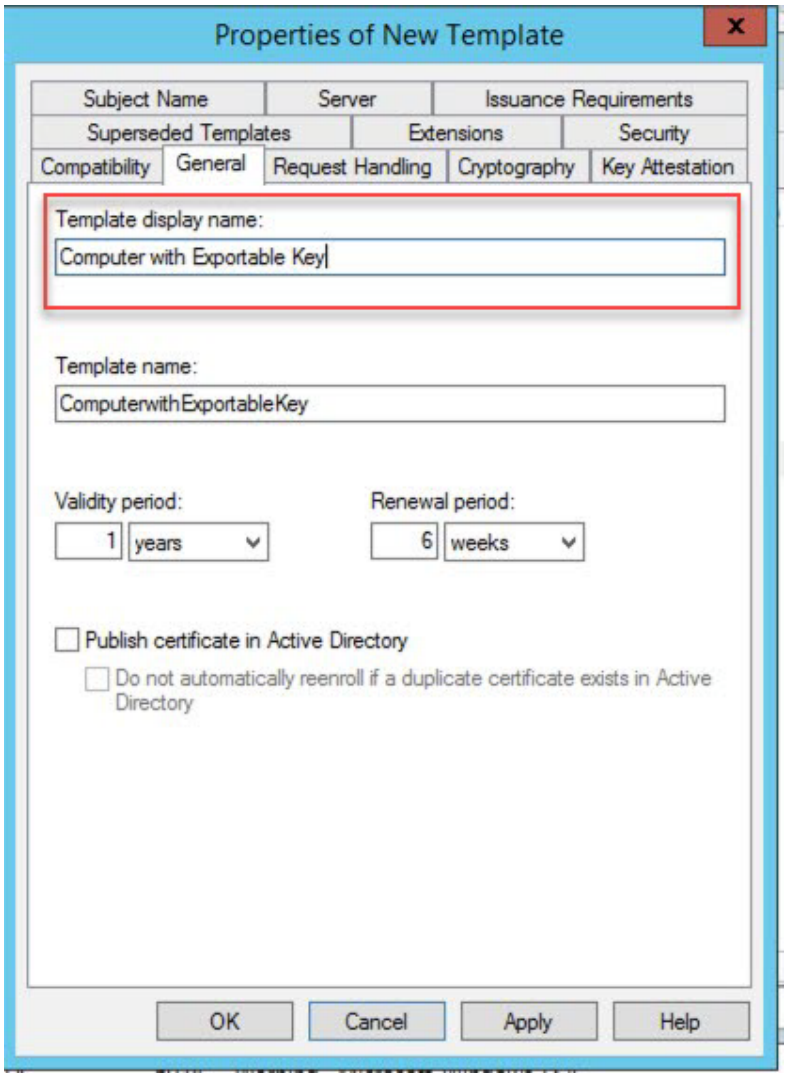
3. Scroll down and right click the **Computer** template and select **Duplicate Template**.
   This opens the new certificate template window.



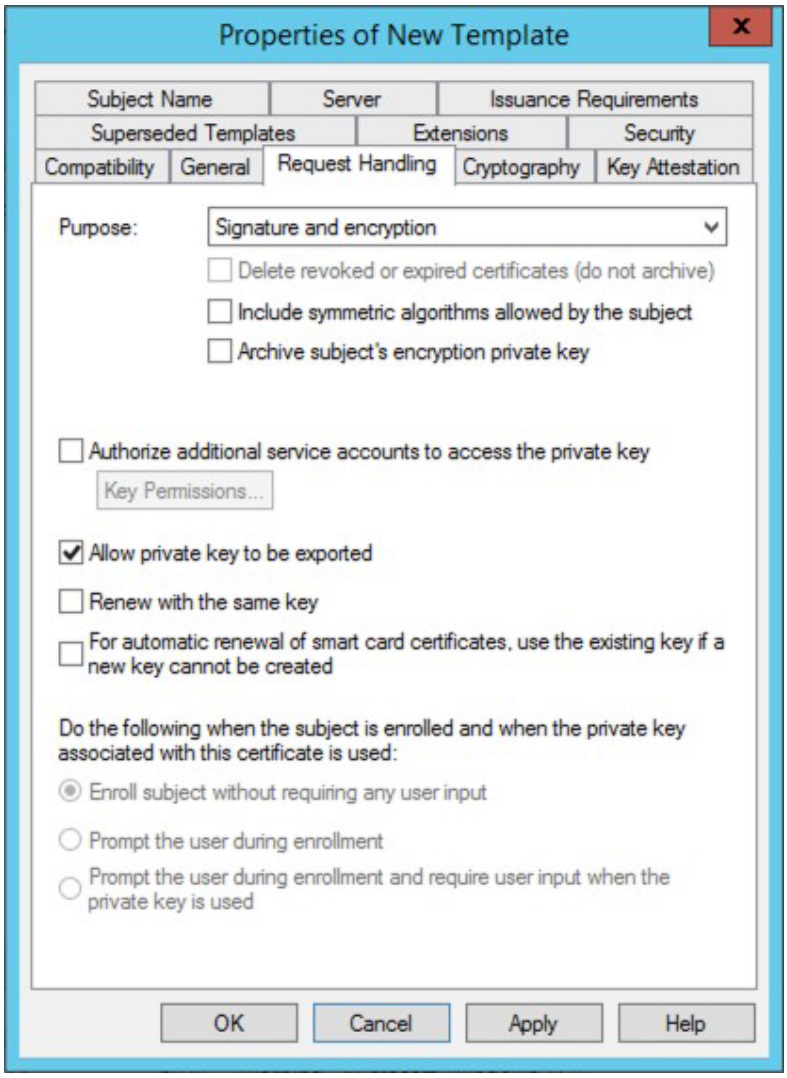
4. Navigate to the **Compatibility Settings** tab:
   - For the **Certification Authority** field, select **Windows Server 2012 R2** or higher.
   - For the **Certificate Recipient fields**, select **Windows 8.1 Windows Server 2012 R2** or higher.



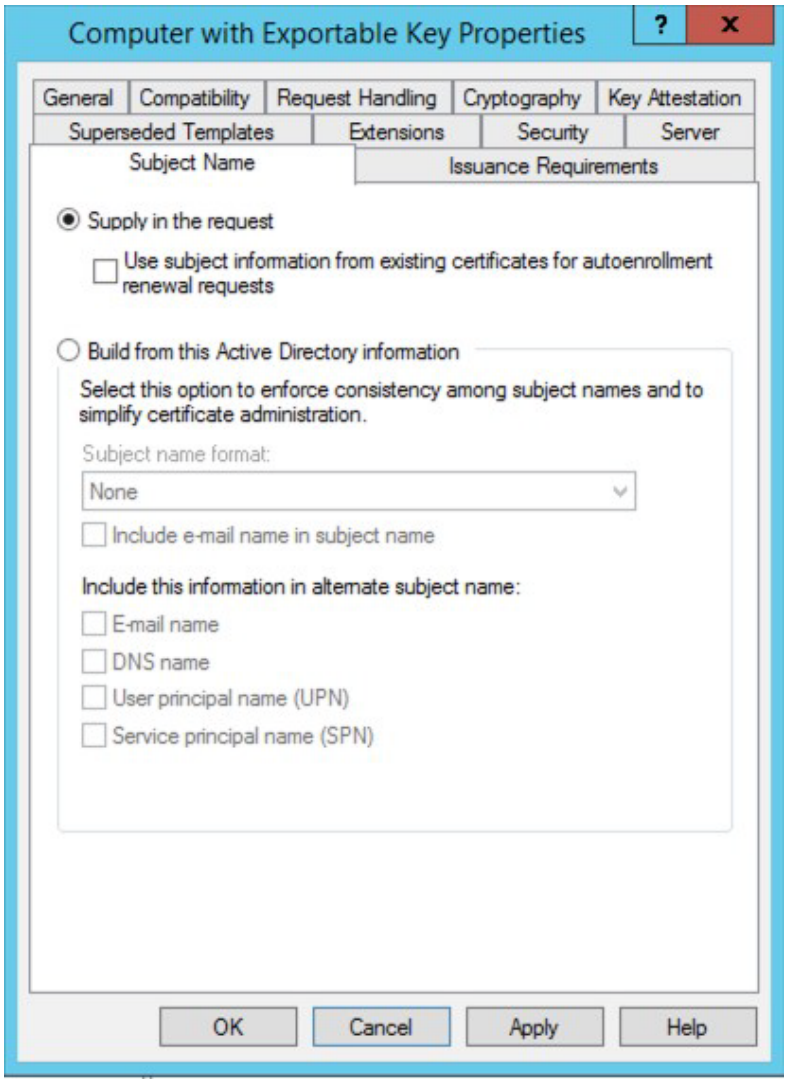
5. Navigate to the **General** tab. For **Template display name**, set it to “Computer with Exportable Key” (no quotes):



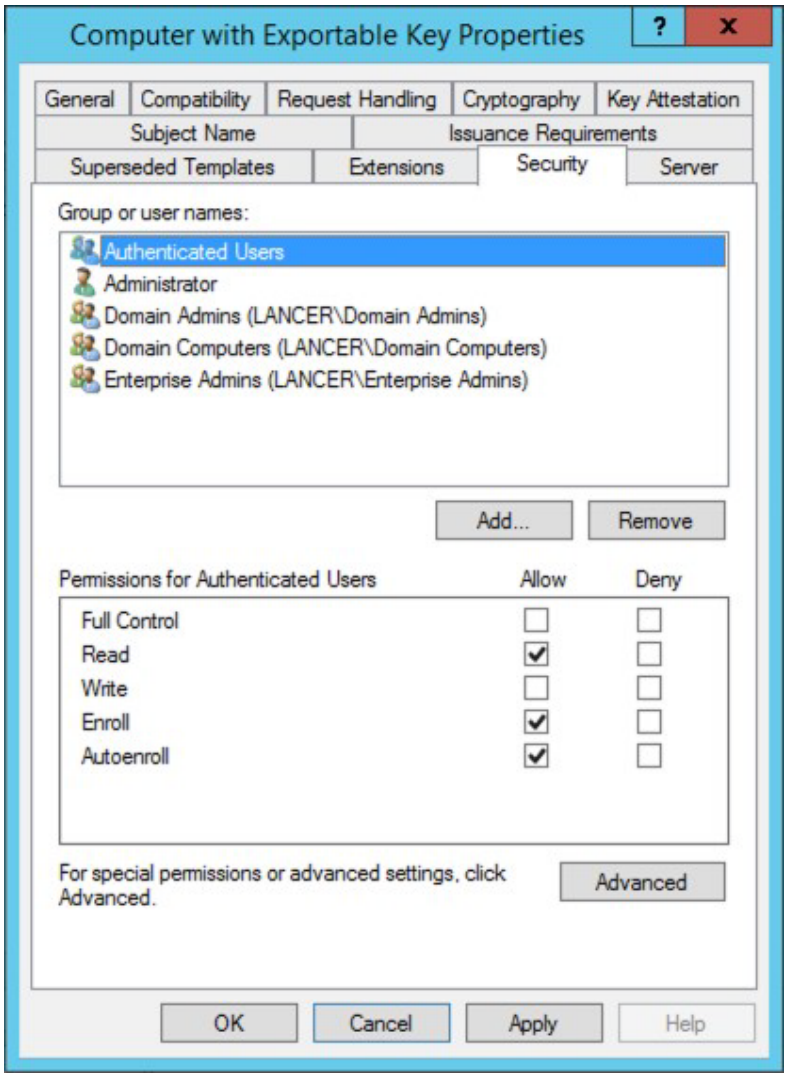
6. Navigate to the **Request Handling** tab and check the checkbox “Allow the private key to be exported.”



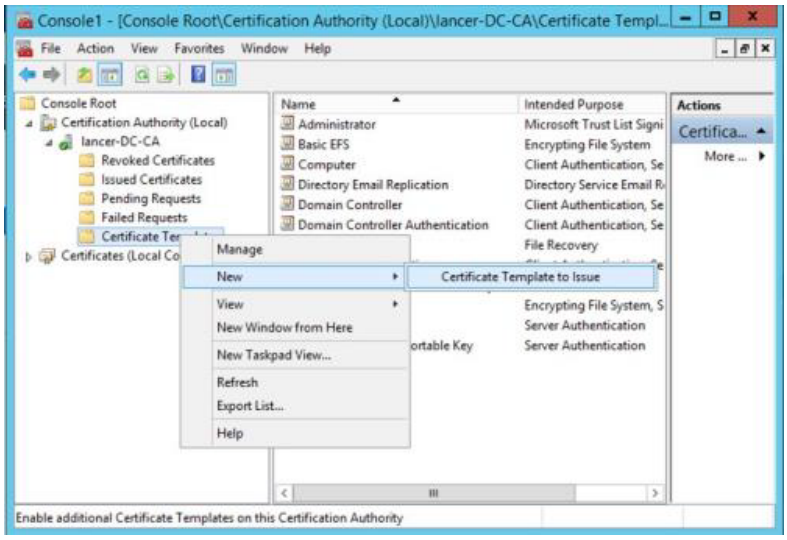
7. Click the **Subject Name** tab and choose **Supply in the Request**:



8. Navigate to the **Security** tab. Here, authenticated users is highlighted. In the lower pane, check the boxes for **Enroll** and **AutoEnroll**.



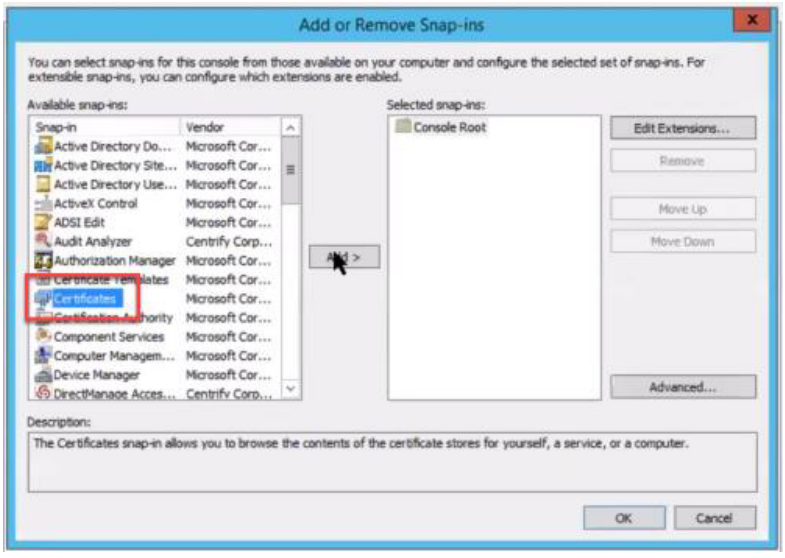
9. Click **OK**. This will save this new **Certificate Template** and close the **Certificate Templates Window**.
10. Back in the **Certification Authority** console, right-click **Certificate Templates** > **New** > **Certificate Templates to Issue**. This opens the **Enable Certificate Templates** window.



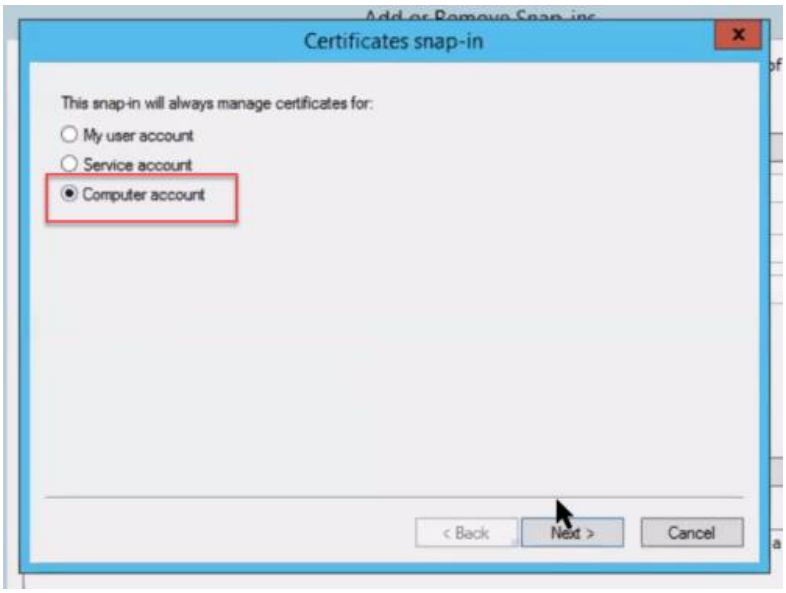
11. Scroll down to **Computer with Exportable Key** and click **OK**. The modified template is now ready for use through group policy.
12. Close the **Certification Authority** console.

To generate a computer certificate for the Delinea Connector

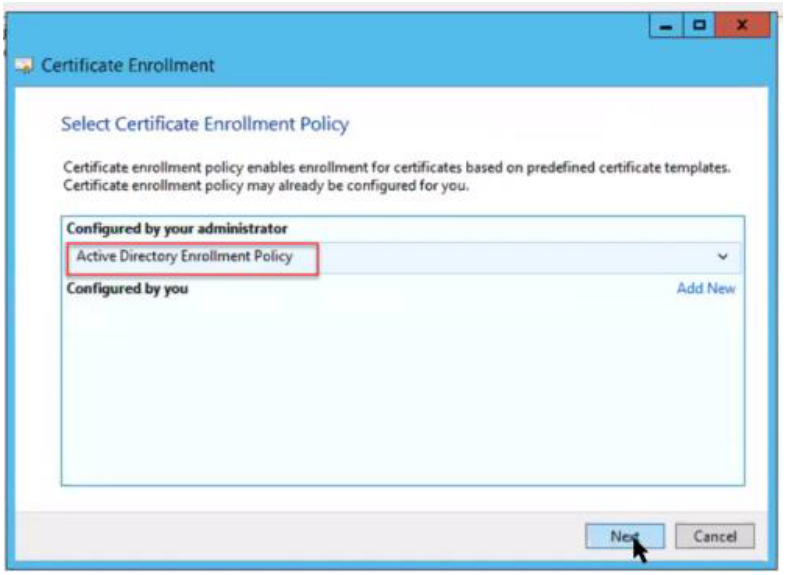
1. In the server where you're going to create the certificate, open the mmc.exe program.
2. In the MMC program, navigate to **File** > **Add/Remove Snap-ins** add the **Certificates (Computer)** snap-in and click **Add**



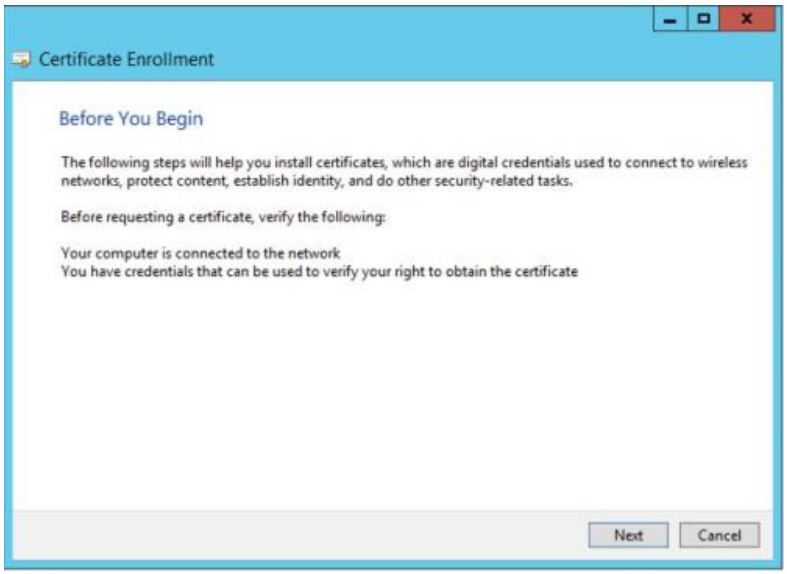
3. For Certificates snap-in, choose **Computer account** and click **Next:**



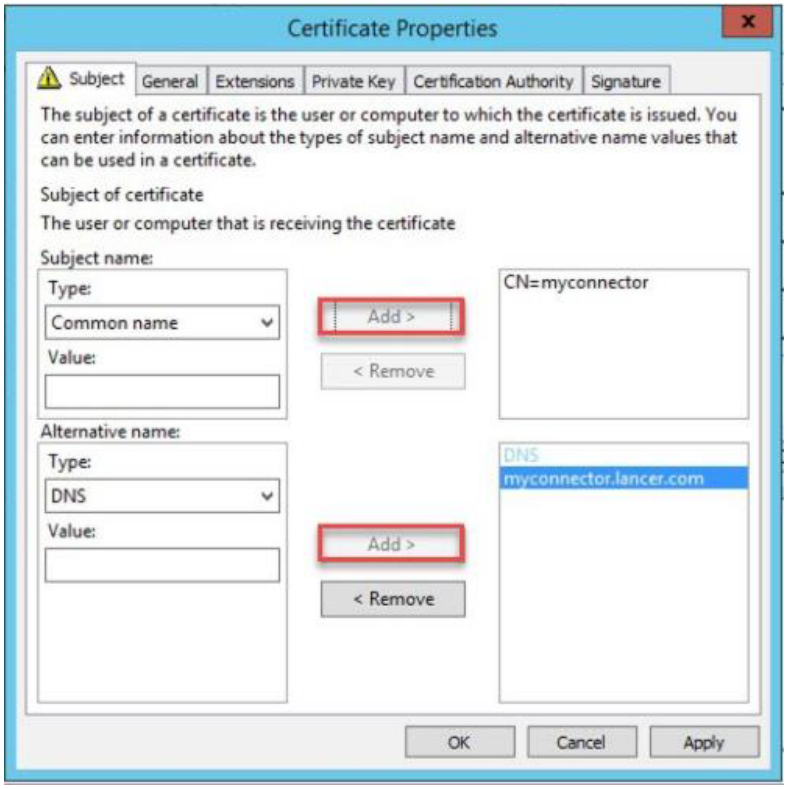
4. For the **Select computer** screen, keep all default and click **Finish** and then click **OK.**
5. Navigate back to the console, and under **Console Root**, right-click **Personal**> **All Tasks** > **Request New Certificate**. Click **Next** on the **Certificate Enrollment** screen. On the **Select Certificate Enrollment Policy** screen, ensure you have **Active Directory Enrollment Policy** and click **Next.**



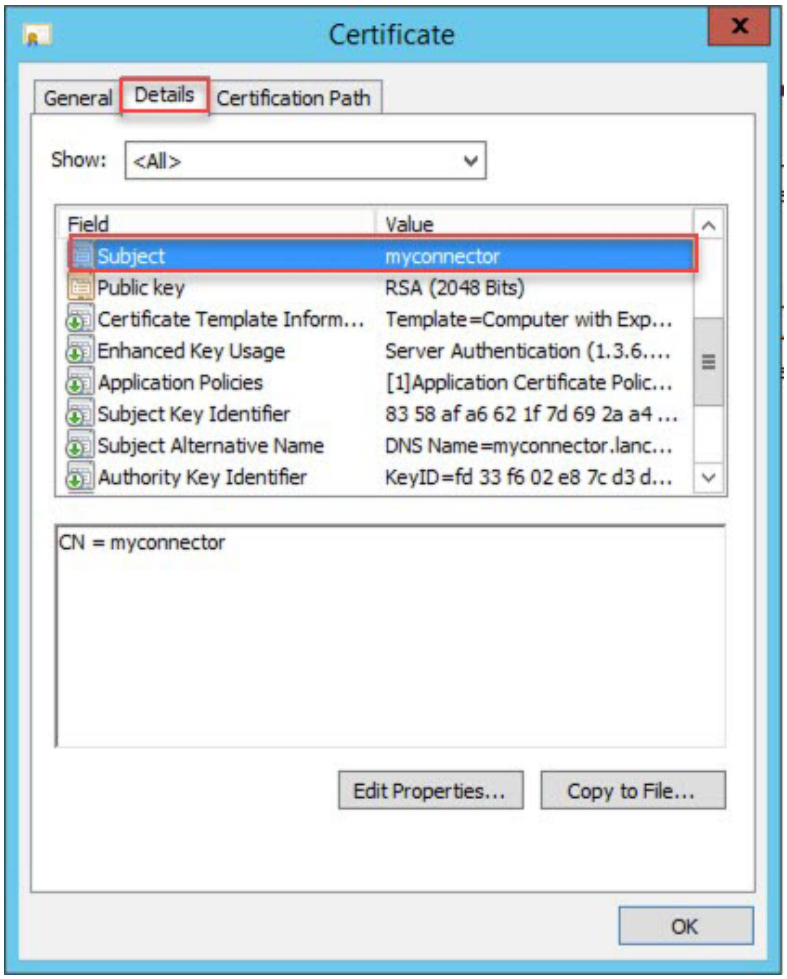
6. For **Request Certificate**, click the checkbox for **Computer with Exportable Key** and click the hyperlink directly beneath the selection entitled **More information is required to enroll for this certificate. Click here to configure settings**.

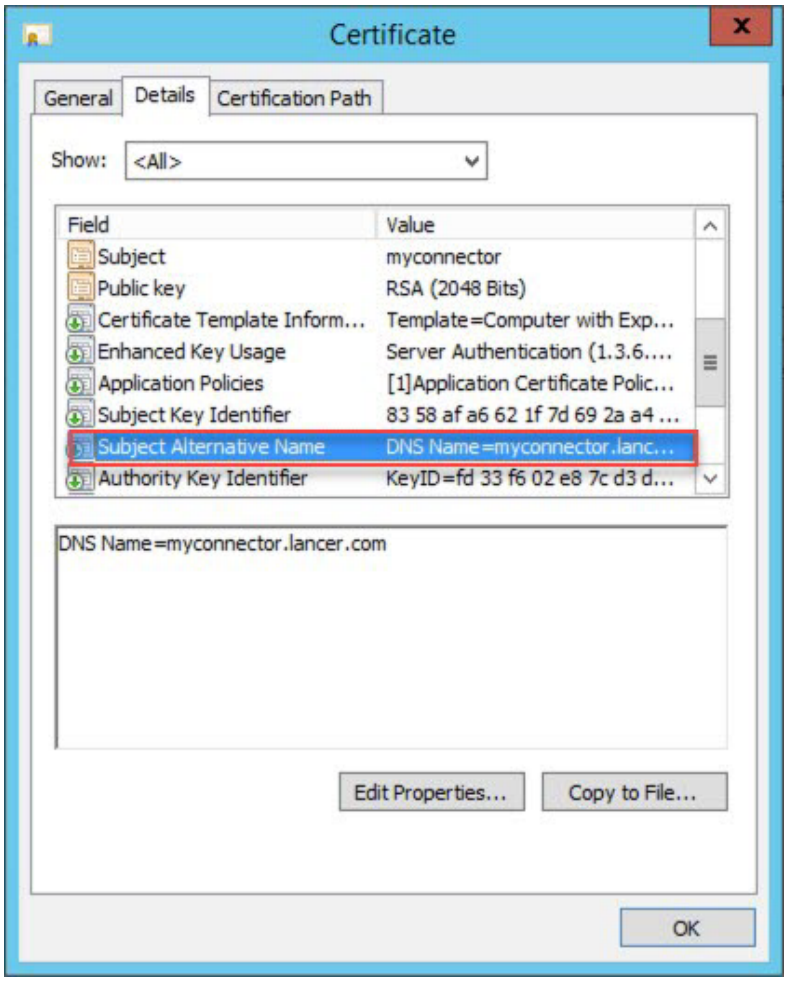


7. Then press **Add** on both **Subject name** and **Alternative name** to move the set values to the right hand side and click **OK**:



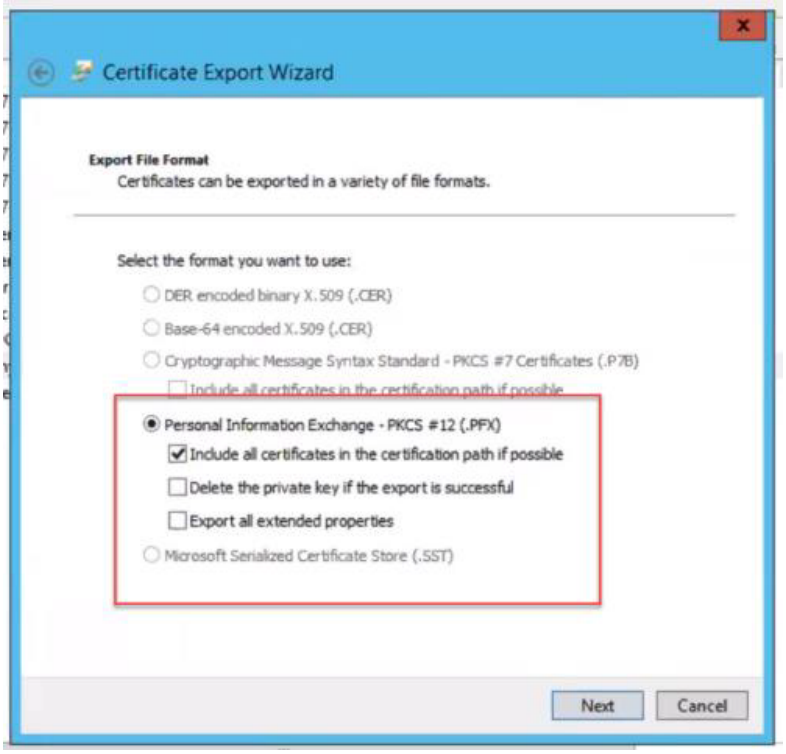
Note: To obtain the **Subject name** and **Alternative name**, click on the certificate details (subject name and subject alternative name) as seen below:


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
myconnector
Public key
RSA (2048 Bits)
Certificate Template Inform...
Template=Computer with Exp...
Enhanced Key Usage
Server Authentication (1.3.6....
Application Policies
[1]Application Certificate Polic...
Subject Key Identifier
83 58 af a6 62 1f 7d 69 2a a4 ...
Subject Alternative Name
DNS Name=myconnector.lanc...
Authority Key Identifier
KeyID=fd 33 f6 02 e8 7c d3 d...
CN = myconnector
Edit Properties...
Copy to File...
OK

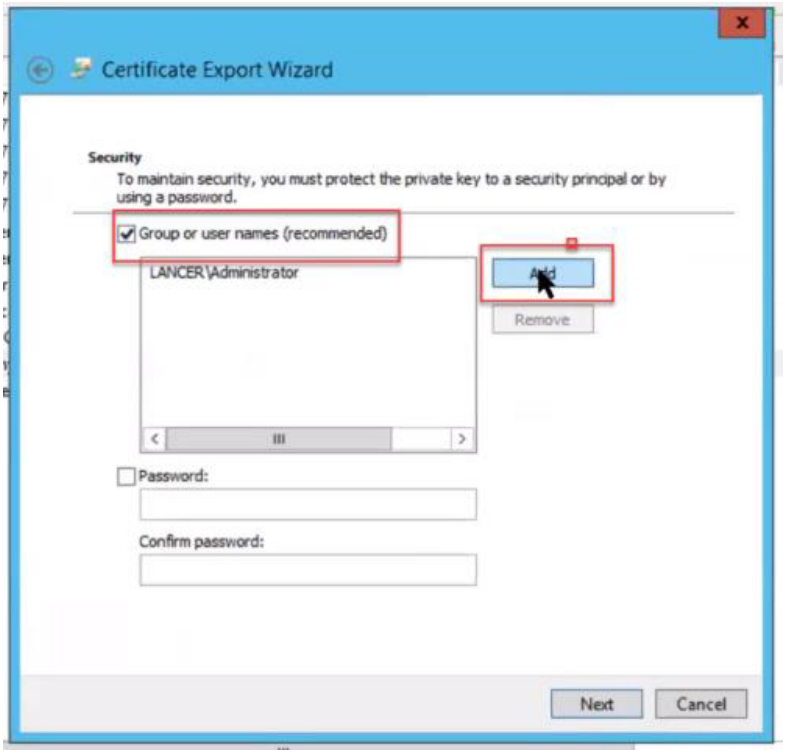


To export the certificate with the private key

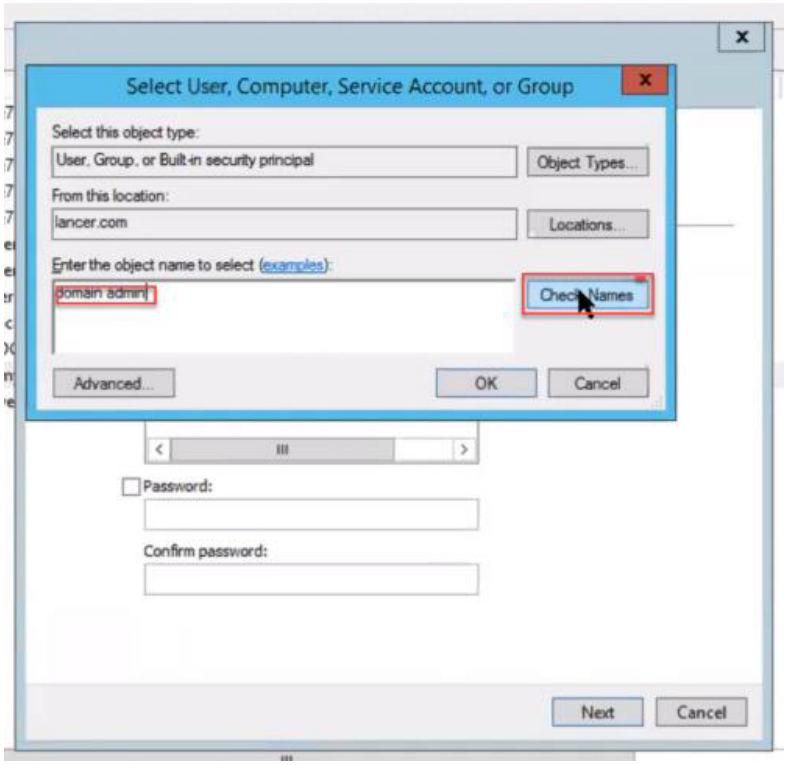
1. Under **Personal** > **Certificates**, right click the Delinea (or the name of the server) Certificate and select **Export**.
2. On the welcome page click **Next**.
3. On the **Export Private Key** screen, select **Yes, export the private key** and click **Next**.
4. For **Export File Format**, keep default (**Personal Information Exchange - PKCS # 12 (.PFX)**) and click **Next**.



5. For the **Security** screen, click the checkbox **Group or user names (recommended)**



and click **Add**. For the **Select User**, Computer, Service Account, or Group screen, in the field **Enter the object name to select (examples)** enter **domain admin** and click **Check Names**:



Click **OK** and click **Next**.

6. For **File to Export**, name the file and click **Save**.
7. Click **Next**. Make a note of this location, you'll need it during Delinea setup (example: `c:\centrify\centrify.pfx`).
8. Lastly, for the **Completing the Certificate Export Wizard** screen, click **Finish**.
   You will see a screen pop up stating the export was successful.
   Click **OK**.

   You use the exported certificate and install it onto the computer where you have installed the cloud connector. For details, see "Importing a Certificate" on page 306.

Select the Client Certificate to Use for the Connector

To ensure secure communication between KeySecure and the Delinea Connector, you need to have a signed client certificate. Depending on your environment and tools available, you might select one of the following options:

- You can create a new client certificate using the KeySecure management console or another tool to use for the Delinea Connector. This option is similar to creating the server certificate except that you select Client for the Certificate Purpose.
- You can use an existing client certificate that you use for other secure services.
- You can use the certificate created by the Privileged Access Service.

The first two options assume you are signing the certificate with a trusted local certificate authority and require you to upload the signed client certificate to the connector. The third option requires you to download the Delinea CA certificate onto the KeySecure appliance. After you have selected an option for obtaining the client certificate, you have all of the information required to configure SafeNet KeySecure as the password storage location for the accounts you add to the Privileged Access Service.

For complete information about installing and configuring a SafeNet KeySecure hardware security appliance, see the **KeySecure Installation and Configuration Guide**.

How to Uninstall the Privileged Access Service Software

You use the Uninstall command in the Windows Control Panel to remove the connector and console extensions.

All of the components are installed under the name Privileged Access Service Management Suite followed by the version number. Uninstalling this program removes all of the Privileged Access Service components installed on the computer. You cannot, for example, delete the connector but leave the console extensions.

If you use just one Delinea Connector uninstalling the Delinea Management Settings from the Active Directory Control Panel terminates mobile device policy enforcement. However, if you uninstall the Delinea Management Suite from one computer but have the Delinea Connector installed on one or more other computers, service is not interrupted. In this case, Privileged Access Service automatically switches to another connector.

To uninstall the Privileged Access Service software:

1. On a Windows computer on which you installed Delinea directory policy service Management Suite, close any open Microsoft Management Consoles, such as Active Directory Users and Computers and Group Policy Management Editor, that may be using the components.
2. Click **Start > Control Panel > (Programs) Uninstall Program**, then right-click Privileged Access Service Management Suite version.
3. Click **Yes** when the confirmation message appears.

   If no Microsoft Management Console applications are open, the installer finishes and removes the Delinea Management Suite software. If applications are open, you are prompted for how to close them.
4. If prompted to close open applications, do the following:
   - Leave the following option selected and click **OK**:

     Automatically close applications and attempt to restart them after setup is complete.
   - If prompted that a Microsoft Management Console application has stopped working, click **Close the program**.

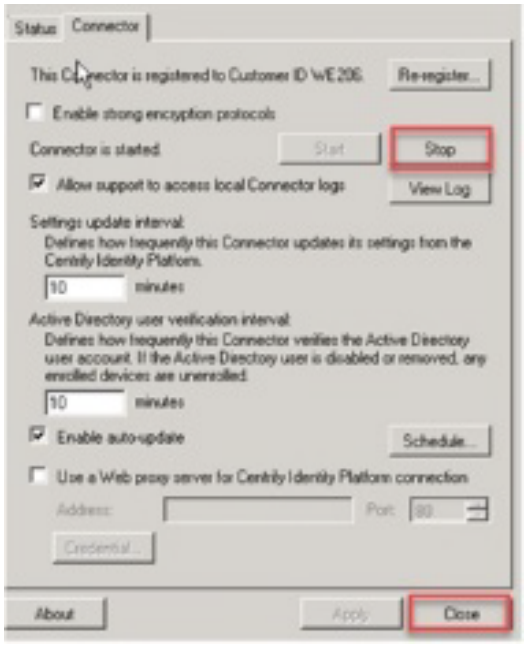
     The connector and, if also installed, the console extensions are now removed from your computer. However, a directory and some files will still reside on your computer. To remove these files, complete the next step.
5. To remove Privileged Access Service related files, navigate to and delete the `C:\Program Files\Centrify` folder.

How to Delete a Connector

You can only delete inactive connectors. You cannot delete an active connector. An inactive connector is one that is offline.

To take a connector offline:

1. Open the Delinea Connector Configuration Program on the connector machine.
2. Click the **connector** tab > **Stop**.

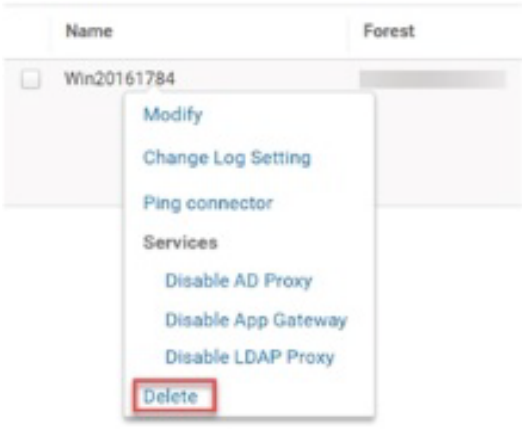


3. Click **Close**.

   When the connector is offline, there is no communication between it and the Privileged Access Service.

To delete a connector:

1. Log in the Admin Portal.
2. Right click the relevant connector and click **Delete**.



The connector listing is removed from the page.

Deleting a connector removes the listing from the Admin Portal page. It does not, however, uninstall the Delinea Connector software from the computer. You can re-activate the connector by re-registering it.

Disk Space Alerts

You get disk space alerts on an Active Directory member server where the Delinea Connector is installed.

Possible Cause

The disk space alerts may be caused by the creation of local user profiles on the host machines running the Delinea Connector. The local user profile can be created for users who have never logged on to the Delinea Connector host. The profiles get created by the Directory Services API when the call for “ChangePassword” is triggered. The call is triggered when **both** of these conditions are met:

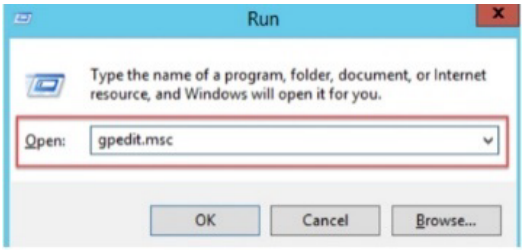
- User uses the self service password reset option from Admin Portal > **Profile** > **Security** tab.
- User has rights to “Logon Locally” to the connector host.

Resolution

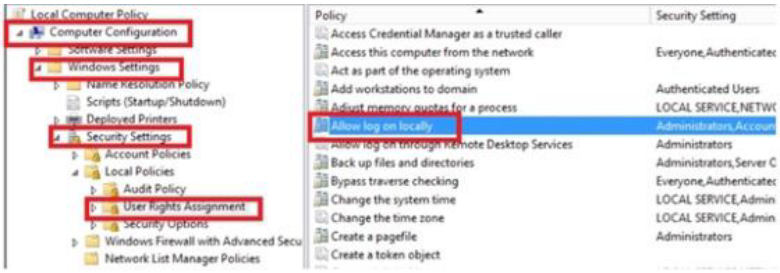
You can prevent the creation of local user profiles by following these procedures. These procedures will not delete the profiles already created; they only prevent the creation of more profiles.

To prevent the creation of local user profiles:

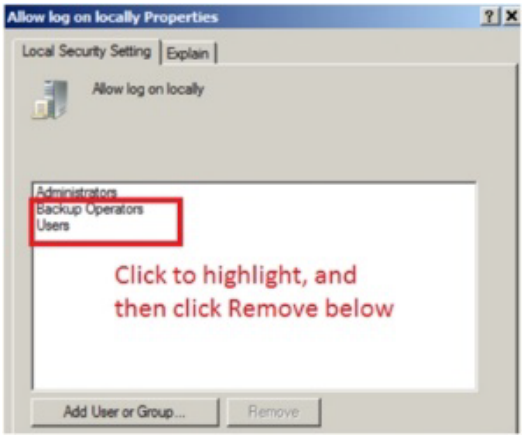
1. Log in as an Administrator and open the Local Group Policy Editor by typing **gpedit.msc** in the Run box.



2. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.



3. Click **Allow log on locally** and remove "Users" and "Backup Operators".



4. Click **Apply**.

Managing Domain Controllers that are Slow to Respond to Requests

When domain controllers are slow to respond to requests, they are ranked lower compared to healthier domain controllers and thus taken out of rotation. As such, the domain controller is not used (unless no other healthy domain controllers are available). The domain controller is reset after discovery.

Adding a Domain Controller Back into Rotation

To be removed from the "penalty box," and added back to rotation -- the domain controller must be discovered. The following are registry keys that you can set to perform advanced configuration of your domain controller searches.

Registry key	Description
AD.SearchOnePenaltyBoxThreshold	This key allows you to specify what percentage of ServerTimeLimit should be spent searching for a single AD entity before the chosen domain controller is put in the penalty box. Default is 25 (25%) - TYPE = **DWORD**.
AD.SearchManyPenaltyBoxThreshold	This key allows you to specify what percentage of ServerTimeLimit should be spent searching for many AD entities before the chosen domain controller is put in the penalty box. Default is 90 (90%) - TYPE = **DWORD**.
AD.ServerTimeoutMax	When performing a "normal" search (not a paged search), this value specifies the maximum amount of time the server should spend searching before returning results (https://docs.microsoft.com/en-us/dotnet/api/system.directoryservices.directorysearcher.servertimelimit?view=netframework-4.8) - TYPE = **DWORD**

Registry key	Description
AD.SearchSizeMax	When performing a "normal" search (not a paged search), this value specifies the maximum number of results that can be returned in a directory search (https://docs.microsoft.com/en-us/dotnet/api/system.directoryservices.directorysearcher.sizelimit?view=netframework-4.8) - TYPE = **DWORD**
AD.PageSizeMax	When performing a paged search, this value specifies the maximum number of objects that can be returned in a paged search (https://docs.microsoft.com/en-us/dotnet/api/system.directoryservices.directorysearcher.pagesize?view=netframework-4.8) - TYPE = **DWORD**
AD.PageTimeMax	When doing a paged search, this value specifies the maximum amount of time the searcher should spend searching for an individual page of results (https://docs.microsoft.com/en-us/dotnet/api/system.directoryservices.directorysearcher.serverpagetimelimit?view=netframework-4.8) - TYPE = **DWORD**
AD.DCPenalityBoxEnabled	This is an on/off switch for the domain controller penalty box feature (default is ON). Set to 0 for off, 1 (or unset) for on. - TYPE = **_DWORD**.

Reference content -- Connector Configuration Program

Initial configuration of the Delinea Connector follows installation with the connector configuration wizard, which launches automatically. To complete the wizard, you must identify a user group whose members can register devices and a container that stores accounts for registered devices. You must also identify a group whose users have permission to manage registered devices and manage the configuration.

The connector configuration program allows you to complete the initial configuration and to make changes when necessary. You can also run this application to monitor the status of your connector.

Privileged Access Service uses all of the available connectors configured for a service. Each server has a connector configuration program that you launch on the computer hosting the connector. Changes made to one connector in an installation (servers registered to the same customer ID), the changes are propagated to all the servers in the installation to ensure that they are all in sync.

The Delinea Connector Configuration Program is installed on any computer where a connector is installed. You can launch it from the Windows Start menu. The application appears as a window with tabbed panels:

- **Status**: Shows server name, Delinea customer ID, and Delinea connection status.
- **Delinea Connector:** Provides connector controls and option settings.

Supporting User Authentication for Multiple Domains

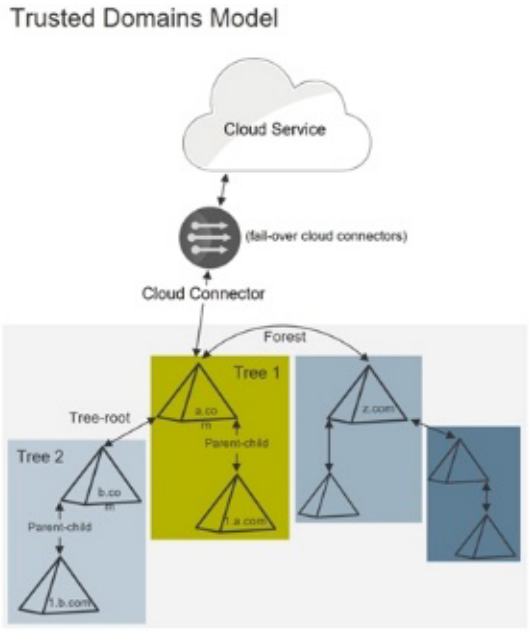
You install the connector on a host Windows computer that is joined to a domain controller to authenticate Privileged Access Service users who have an account in that domain. If you want Privileged Access Service to authenticate users in other domains, there are two connector installation models—which one you use depends upon whether the accounts are in trusted domains in a single forest or in multiple, independent domain trees or forests.

Note: If all of your Privileged Access Service users have their accounts in a single domain controller, you can skip this topic.

Configuring Authentication for Trusted Domains

You use this model when the users' Active Directory accounts are in domains with domain controllers that have a two-way, transitive trust relationship with the domain controller to which the connector is joined.

In this model, you have a single connector for the entire domain tree or forest. Privileged Access Service communicates through this connector for all authentication requests. When the user account is in another domain, the authentication requests are handled according to the tree-root, parent-child, forest, and shortcut trust relationship settings between the domain controllers.



If you are using Active Directory for device and policy management, all object management communications are done through the same connector as well.

By default, two-way transitive trusts are automatically created when a new domain is added to a domain tree or forest root domain by using the Active Directory Installation Wizard. The two default trust types are parent-child trusts and tree-root trusts. When you configure the trust relationship, be sure to select Forest trust. This establishes a transitive trust between one forest root domain and another forest root domain. See How Domain and Forest Trusts Work in Microsoft TechNet for more about trust relationships.

IMPORTANT: For tenants created after the Privileged Access Service 17.1 release, the connector by default does not perform cross forest user lookup from a local forest. To enable this functionality, contact Delinea Support.

After you install the first connector, you should install one or more on separate host computers. The host computer for each connector must be joined to the same Active Directory domain controller. See "Creating Administrator Consoles and Adding Additional Connectors" on page 451 for the details.

Privileged Access Service automatically creates a login suffix for the domain to which the host computer is joined plus all of the domains that the connector can see. Which domains can be seen depends upon two criteria:

- The trust relationship between the domain controllers.

  Only domain controllers with a two-way transitive trust meet this criteria

- The connector's user account permissions.

  By default the connector is installed as a Local System user account on the Windows host. (See "Permissions Required for Alternate Accounts and Organizational Units" on page 412 for more information.) The permissions you grant to this account can affect its ability to see other domains.

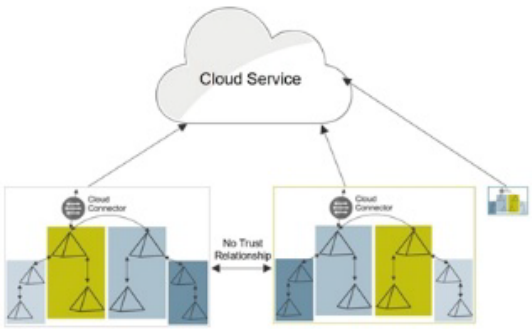
  Note: When the Admin Portal searches Active Directory domains for users and groups (for example, when you are adding a user or group to a role), it only searches the Active Directory Users container in the domain controllers that can be seen by the connector.

Independent Domains in Multiple Forests

You use this model when the users' Active Directory accounts are in independent domain trees or forests; that is, there are domain controllers that *do not* have a two-way, transitive trust relationships with each other.

In this model, you have a separate connector for each independent domain tree or forest. Privileged Access Service picks which connector to use for the authentication request based on the login-suffix-to-domain mapping it creates and maintains. When the user account is in the connector's domain controller, the authentication requests are handled according to the tree-root, parent-child, forest, and shortcut trust relationship settings between the domain controllers in that forest or domain tree.

Independent Domains Model



After you install the first connector for each independent domain tree or forest, you should install one or more on separate host computers for each one. The host computer for each connector must be joined to the same Active Directory domain controller as the initial connector for this tree or forest. See "Creating Administrator Consoles and Adding Additional Connectors" on the next page for the details.

Privileged Access Service automatically creates a login suffix for the domain to which the host computer is joined plus all of the domains that the connectors for each independent domain can see.

When Admin Portal searches Active Directory domains for users and groups (for example, when you are adding a user or group to a role), it only searches the Active Directory Users container in the domain controllers that can be seen by the connectors. Which domains can be seen depends upon two criteria:

The trust relationship between the domain controllers.

Only domain controllers with a two-way transitive trust meet this criteria. When you configure the trust relationship, be sure to select Forest trust. This establishes a transitive trust between one forest root domain and another forest root domain. See How Domain and Forest Trusts Work in Microsoft TechNet for more about trust relationships. The connector's user account permissions.

By default the connector is installed as a Local System user account on the Windows host. The permissions you grant to this account can affect its ability to see other domains. See "Permissions Required for Alternate Accounts and Organizational Units" on page 412 for more information.

If you are using this model, use the Delinea directory policy service to set mobile device policies (see "How to Select the Policy Service for Device Management" on page 738 and Privileged Access Service roles to enable users to register devices.

Modifying the Default Connector Settings

You use the Delinea Connector Configuration Program to modify the default setting. See "Reference content -- Connector Configuration Program" on page 448 for the description of each tab and how to modify the default settings.

There are several default settings you may need to change right after you install the connector:

Setting	Tab	To Do This
Enable auto-update	Delinea Connector	Configure the connector to automatically poll Privileged Access Service for software updates and install them. You can also specify the polling-update windows.
Active Directory user verification interval	Delinea Connector	Set the polling period between queries for updates to active Active Directory user accounts.
Log settings	Logging	After you install a connector, you should configure the connector to log activities to help in troubleshooting in case you have any problems. Go to this tab to enable logging.

Creating Administrator Consoles and Adding Additional Connectors

You use the same Delinea Management Suite installer to install the additional connectors for load balancing and failover and administrator consoles to manage users, devices and group policy objects.

About Load Balancing and Failover

You should configure one or more connectors to provide continuous up time for Privileged Access Service services. Each connector you add is listed in Admin Portal on the Settings page in the Delinea Connector tab.

Privileged Access Service provides load balancing among all connectors with the same services installed. For example, when a request comes in, Privileged Access Service routes the request among the available connectors. If one connector becomes unavailable, the request is routed among the other available connectors providing automatic failover.

Installing Additional Connectors

You use the same procedure to download the installation wizard to the host computer and then run the wizard to install and register additional connectors. After you install and register the connector, it is added to the Delinea Connector page.

Note: The host computer must be joined to the same Active Directory domain controller as the first connector in the same trust domain or forest.

Creating a Privileged Access Service Administrator Console

You use the same procedure to download the installation wizard to the host computer and then run the wizard. However, you do not install the connector. Instead, you install either or both of the console extensions.

Note: The host computer must be joined to the same Active Directory domain controller as the connectors in the same trust domain or forest.

Using the Status Tab

The **Status** tab displays the following read-only information about the connector:

- **Server name** displays the assigned name of this connector.
- **Customer ID** displays the customer ID under which this connector is registered. You can install multiple connectors using the same customer ID for load balancing and failover. All active connectors are used by Privileged Access Service.

  Note: Do not change this field.
- **Delinea Connector is started|stopped** shows whether the connector is started (running) or not.
- **Connection to Privileged Access Service** shows the date, time, and result of the last connection to Privileged Access Service.

Using the Delinea Connector Tab

The **Delinea Connector** tab reports the customer ID under which the Delinea Connector is registered and whether or not the server is started. It also offers the following controls:

The **Re-register** button starts the Delinea Connector configuration wizard and allows you to re-register this connector. Generally, you re-register the connector under the same customer ID, and then only if the connector is having difficulty communicating with Privileged Access Service and customer support recommends that you re-register to address the issue.

Note: Re-registering under a different ID can destabilize your environment and should be done **only** after consulting with customer support. Changing the ID moves the connector from one installation to another. If the connector is the only server in an installation, removing the server from the installation will cause any device registration to the installation to fail, and registered devices will no longer receive policy changes.

Click **Start** to start the connector if it's stopped.

Click **Stop** to stop the connector if it's running.

Select **Allow support to access local connector logs** to give the identity provider the ability to open the connector log files. These files can help resolve a problem and are the only files the service provider can open. The default is selected.

Click **View Log** to view the connector log. "How to Change Connector Log Settings" on page 420.

Use the **Settings update interval** text box to set the number of minutes this connector takes between checks on connector settings with Privileged Access Service.

When any connector in an installation changes its settings, it sends those settings to Privileged Access Service. When a connector checks settings with Privileged Access Service, if there were new settings reported from any of the other connectors in the installation, the checking connector downloads and accepts those settings. This ensures that all connector is in an installation have the same settings.

Use the **Active Directory user verification interval** text box to set the number of minutes this connector takes between checks for active AD user accounts. When the connector checks Active Directory user accounts, it contacts Active Directory/to see if the user account listed for each registered device is active. If a device's associated user account is not active (is disabled or removed), Privileged Access Service un-registers the device.

Select the **Enable auto-update** check box to turn on automatic update for the connector. When auto-update is on, the connector checks with Privileged Access Service periodically to see if there is a connector update. If there is, the connector downloads and installs the update, then restarts. This ensures that connector software is up-to-date. We recommend that you enable this option. See "How to Auto-update Connector Software" on page 421 for the details.

Select **Use a web proxy server for Privileged Access Service connection** check box if your network is configured with a web proxy server that you want to use to connect to Privileged Access Service. Note that the web proxy must support HTTP 1.1 for a successful connection to Privileged Access Service. After you select this option, enter the following information to enable the web proxy connection:

- **Address** is the URL of the web proxy server.
- **Port** is the port number to use to connect to the web proxy server.
- Click **Credential** to enter the user name and password for an account that can log in to the web proxy server.

Cloud Suite and Connector Outbound Network Firewall Requirements

Firewall and External IP Address Requirements

All connections to the internet made by Privileged Access Service (including Delinea Connector and mobile management) are outbound in nature. No internet facing ingress ports are required.

Note: To view the firewall rules, see Review the Firewall Rules for more information.

All outbound connections are made by way of TCP to either port 80 or 443 and should not have any restrictions.

To provide the redundancy and availability of an always available Privileged Access Service, the destination resource, IP address, and host for outbound connections will vary over time amongst thousands of addresses. Additionally, the range of which also changes as new resources are provisioned or removed.

Note: Use of deep packet inspection filtering of HTTPS or SSL traffic by web proxies or security software may cause connectivity issues with Privileged Access Service. In all cases, the ports and addresses discussed below should be excluded from packet inspection to allow for normal service operation.

Option 1: Whitelist Source

Given the variability of connection targets, the simplest whitelist configuration is typically one where filters are based on the traffic source. Specifically, it relates to configurations where you allow all outbound traffic from the host machine and account running the Delinea Connector and for outbound requests made by iOS, Android, and Mac clients. This whitelist may be scoped at the machine, or machine + account, or machine + account + process level depending on the feature set of the security appliance or process in place.

Option 2: Whitelist Source Ports

You can also use a whitelist configuration where all outbound traffic on ports 80 and 443 is allowed from the host machine and account running the Delinea Connector, as well as outbound requests made by iOS, Android, and Mac clients. This whitelist may be scoped at the machine, or machine + account, or machine + account + process level depending on the feature set of the security appliance or process in place.

Option 3: Whitelist Destination

If destination whitelisting is required, you can whitelist outbound ports or TCP Relay IP ranges.

Port numbers	Resource
443	`\*.my.centrify.net` (if you need to whitelist your tenant URL)
80	`privacy-policy.truste.com`
80	`ocsp.digicert.com`

If whitelisting an entire domain (*.centrify.com) is not acceptable per security policy, then you need to whitelist the TCP Relay IP ranges for your relevant Privileged Access Service tenant region. Refer to https://www.microsoft.com/en-us/download/confirmation.aspx?id=56519 for a list of Microsoft Azure datacenter IP ranges by region.

Tenants

If your tenant is on third-party servers, then you need to whitelist the IP ranges for your relevant Privileged Access Service tenant region. Download the relevant file that contains the IP address ranges information. For AWS you can download them from https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html.

Use the table below to find the TCPRelay IP address ranges for each tenant's region:

Region	IP Address Range
US East	3.14.30.0/27 (adding 4 May 2019) 13.58.135.200/29 18.216.13.0/26 34.236.32.192/26 34.236.241.0/29
US West	13.56.112.160/29 13.56.112.192/26 34.215.186.192/26 34.214.243.200/29 35.89.238.96/28 35.89.238.128/27
Canada	35.183.13.0/26 35.182.14.200/29
Europe	18.194.95.128/26 18.194.95.32/29 34.245.82.128/26 34.245.82.72/29
Brazil	18.231.105.192/26 18.231.194.0/29
Australia	13.211.166.128/26 13.211.12.240/29
Singapore	13.250.186.64/26 13.250.186.24/29
London	3.10.127.0/27 3.10.127.64/26 35.176.92.128/26 35.176.92.72/29

For additional information about whitelisting a tenant for use with web proxies and firewalls, see KB-13446.

Working with Resources and Remote Clients

You can add resources (systems, databases, domains, accounts, secrets, SSH keys, and services) to the Admin Portal and manage access to those resources.

For most systems that you add, you can log on and perform remote operations through secure shell (SSH) or remote desktop (RDP) sessions.

Accessing Resources

To access the accounts page, navigate to **Resources > Accounts**. Once there, you can perform the following tasks:

- "Identifying Favorites" on page 458
- "Selecting Account Actions" on page 459

Accessing Accounts

To access the accounts page, navigate to **Resources** > **Accounts**. Once there, you can perform the following tasks:

- "Identifying Favorites" on page 458
- "Selecting Account Actions" on page 459

Account Types

Accounts are associated with targets, and therefore policies:

- Also appear by target type.
- Some policies can be overridden per target.

The account policy types are:

- Checkout lifetime
- Password checkout challenge rules
- Secret access key checkout challenge rules
- Enable periodic password rotation
- Password complexity profile
- Domain administrative account

Checkout Lifetime

The maximum number of minutes administrators are allowed to have a password checked out. After the number of minutes specified, the Delinea PAS automatically checks the password back in. The minimum checkout lifetime is 15 minutes. If the policy is not defined, the default checkout lifetime is 60 minutes.

You can extend the checkout time for a password as long as you do so before the initial checkout period expires. For example, if the maximum checkout lifetime is 60 minutes and you extend the checkout time before the 60 minute period is over, the password expiration is reset to the 60 minute checkout lifetime.

For more information about configuring the Checkout lifetime policy, see "Extend the password checkout time."

Password Checkout Challenge Rules

You can configure authentication rules and authentication profiles to protect access to the account password for specific accounts. Based on the rules you define, users attempting to check out the password for an account with access to a specific system might be required to provide a password, enter the passcode from a text message, or answer a phone call to authentication their identity. The authentication rule defines the conditions for when a

specific authentication profile should be used. The authentication profile defines the types of challenges presented and whether one factor or two factor authentication is required. You can also define a default authentication profile to use if the conditions you specify for the checkout rules are not met.

If you don't create any authentication rules or authentication profiles for password checkouts, users with the appropriate permission can check out stored account passwords without being challenged to re-authenticate their identity or provide multi-factor authentication.

Secret Access Key Checkout Challenge Rules

If you have the Checkout permission, you can check out the password for a stored account to use it for access to a system. When you check out a password, you choose whether to display or copy it to the clipboard for use.

Note: Show Password is only active for 15 seconds. Delinea PAS will hide the password after 15 seconds as a security measure.

Enable Periodic Password Rotation

Select Yes if you want to rotate managed passwords automatically at the interval you specify. Select No if you want to prevent password rotation for the selected system.

If you select Yes, you should also specify the password rotation interval in days. Type the maximum number of days to allow between automated password changes for managed accounts. You can set this policy to comply with your organization's password expiration policies. For example, your organization might require passwords to be changed every 90 days. You can use this policy to automatically update managed passwords at a maximum of every 90 days. If the policy is not defined, passwords are not rotated according to the setting in Settings > Resources > Security Settings tab.

Password Complexity Profile

Select an existing password generation profile or add a new profile for the selected system. If you don't select or add a profile, the default password generation profile for the system type is used. For more information about adding and editing password complexity profiles, see "Configuring Password Profiles" on page 751.

Domain Administrative Account

A domain administrative account enables Delinea PAS to:

- Unlock a domain account if needed.
- Reset the domain account password, in case the password does not match what is stored.

The domain administrative account is also used in the zone workflow feature to update account domain objects

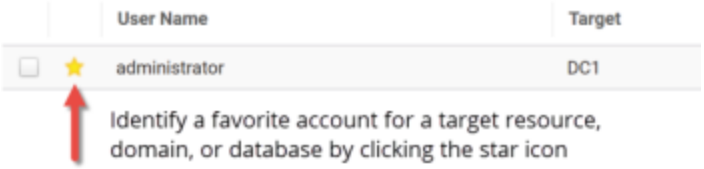
Without a policy, a customer can only have one domain administrative account per domain. This means the account must have permissions for all the domain accounts.

With a policy, multiple domain administrative accounts are enabled. Therefore a customer can have a different administrator for each set of accounts, reducing the quantity of granted permissions to each domain administrative account.

See "Setting Domain Admin Accounts" on page 493 for more information.

Identifying Favorites

As you add accounts to the Privileged Access Service, you might find it convenient to identify the ones you work with most frequently as favorites. You can identify accounts as your favorites by selecting the appropriate Local Accounts, Domain Accounts, or Database Accounts filter, then clicking the star icon next to the account name.



For more on favorite accounts, see "Filtering Favorite Accounts" below

Filtering Favorite Accounts

After you identify favorite accounts, you can filter the accounts listed on any tab to only display the accounts that you work with most often. Identifying an account as a favorite also adds that account to the workspace you see when you click the Workspace tab, enabling you to see activity and take action at a glance without navigating to the full list of local, domain, or database accounts that have been added to the Privileged Access Service.

Justifying Accounts

When the Justification Policy is enabled, prior to the login / checkout process users will see a prompt for Justification only within the UI.

Note: If you directly invoke the login / checkout APIs scripts (not through the UI), justification is not applicable, regardless if the policy is enabled or not.

Justification-Policy-Enabled Login Flow Example

The justification login flow occurs after any account action such as:

- Select / request account
- Enter account
- Use My Account
- Use account-name

The login flow also occurs after any login action from a system local account.

The justification login flow:

1. A dialog box appears, prompting the user to enter a reason / justification with Continue and Cancel options.

   Note: The **Continue** option is highlighted once the you enter the reason / justification text.

2. Once **Continue** is selected, the dialog closes and the normal login flow continues.

The checkout flow occurs after any checkout action:

1. A dialog box appears, prompting the user to enter a reason / justification with Continue and Cancel options.

   Note: The **Continue** option is highlighted once the you enter the reason / justification text.

2. Once Continue is selected, the dialog closes and the normal checkout flow continues.

   Note: The justification dialog will happen prior to any MFA requirements.

Justification Policy Options

The prompt for justification occurs as follows:

- **System Policy** – Yes / no/ cancel prompt during interactive checkout and login operations.
- **Account Policy** - Yes / no/ cancel prompt for during interactive checkout operations.
- **System Set Policy** – Yes / no/ cancel prompt during interactive checkout and login operations.
- **Account Set Policy** - Yes / no/ cancel prompt during interactive checkout operation.
- **Global System Policy** – Checkbox prompt during interactive checkout and login operations.
- **Global Account Policy** - Checkbox prompt during interactive checkout operations on all accounts.
- **Policy Summary** - Shows the state of the policy and inheritance.

Selecting Account Actions

You can select an account to work with by clicking anywhere in the row that contains the account name to display the account details or by clicking the check box for a row. Selecting an account displays the Actions menu from which you can select the action you want to perform.

The actions available depend on the type of account you have selected and the permissions you have been granted. For example, you might see some or all of the following actions on the Actions menu:

- Login to log on to the target system remotely using the selected account and stored password.
- Checkout to check out the password for the selected account.
- Extend to extend the check out time period.
- Check-in to check in the password for the selected account.
- Manage accounts to convert unmanaged accounts into managed accounts. If you are converting a single account and it doesn't have a password configured, you are prompted to enter a password for the selected account. If you select multiple accounts, Privileged Access Service sends an email notifying you of the success/failure of the multiple account management task. The Managed column on the Accounts page indicates the managed accounts. To convert all accounts associated with a set to managed, see "Managing accounts in a set".
- Update Password to update the password stored in the Privileged Access Service for an account.
- Rotate Password(s) to change the password stored in the Privileged Access Service for managed account(s) immediately without waiting for the rotation period to expire. This action is only available if the selected accounts

are accounts with a managed password. If you select multiple accounts, Privileged Access Service sends an email notifying you of the success/failure of the multiple account rotate password task. To rotate all account passwords associated with a set, see "Rotating passwords in a set on demand."

- Set as Admin Account to identify the selected account as a local administrative account.
- Clear as Admin Account to remove the selected account as a local administrative account.
- Add to Set to add the selected account to a new or existing set.
- Verify Credential to make sure the selected account credential (password or SSH key) in Privileged Access Service is in sync with the domain controller credential. Credential verification is performed when Verify Credential is selected from the Actions menu, when the account credential is changed, when an account or administrative account is added, and when resolving an account. The Last Verify Result column on the Accounts page displays nothing if the last credential verification for the account was successful. If the credential verification for the account failed for any reason the column displays Failed, Missing Credential, or Unknown. The Last Verify column on the Accounts page displays the date and time of the last credential verification.
- Show Offline Passcode to get a code to log into an offline system.
- Delete to remove the selected account from the Privileged Access Service.
- Unlock Account to manually unlock the selected account. This option is only visible if the user has the Unlock Account permission, and if the domain the account belongs to has an administrative account defined and has the Enable manual account unlock using administrative account policy enabled. To unlock an account, the user selecting the account must have the Unlock Account permission in the domain the account belongs to. For more information, see Assigning permissions and "Enabling Manual Account Unlock" on page 491.
- Launch to launch the specified application. If you have desktop applications configured and the system is referenced in the Command Line field, then you will see the launch action for that application. See "Adding Desktop Apps Using the Admin Portal" on page 932 for information on configuring desktop applications.

If an account is configured to require the approval of a designated user or role, you might see the Request Login or Request Checkout actions. Selecting Request Login or Request Checkout sends an email request to the designated user or to the members of a designated role for approval. If your request is approved, you have limited period of time to take the action you requested.

The steps for checking out, checking in, or updating a password are the same whether you start from a system, domain, database, service, or account. Only the navigation to where you find the accounts listed and the specific tasks you see listed on an Actions menu vary based on where you are.

For more information about performing the account-related tasks, see the following topics:

- Checking out Account Passwords
- Extending Password Checkout Time
- "Checking in a Password from the Workspace" on page 1052

For more information about configuring, requesting, and responding to access requests, see "Request and Approval Workflow Overview" on page 774.

Account Password Checkout

When you add accounts to the Privileged Access Service, you store the passwords for those accounts securely in a local repository, in the Privileged Access Service, or in an external key management appliance.

If you have the Checkout permission, you can check out the password for a stored account to use it for access to a system, domain, or database. When you check out a password, you choose whether to display or copy it to the clipboard for use. The password remains checked out until either you check it back in or the Privileged Access Service checks it automatically.

The maximum length of time you are allowed to keep a password checked out is configured using a system, domain, database, or account policy. However, you can extend the checkout time for a password that is currently checked out, if needed. For more information about extending the checkout time, see "Extending the password checkout time."

To check out an account password:

1. In the Admin Portal, click Resources, then click Accounts to display the list of accounts.

   You can check out an account password from any list of accounts. For example, the action is available if you are viewing the list of accounts for any specific system, domain, or database. Selecting Accounts is simply the most direct path to performing this task.
2. Type a search string or select a filter to display local accounts, domain accounts, or database accounts.
3. Select an account to display the account details.
4. Click **Permissions** to verify you have the Checkout permission.

   You must have the Grant permission to verify permission settings. If you are a member of the System Administrator role, your user account has this permission by default.
5. Click the Actions menu, then click **Checkout** or **Request Checkout**.

   If the account is configured to require the approval of a designated user or role, click **Request Checkout** to request access from the designated user or role. If your request is approved, you have limited period of time to check out the account password. For more information about the “request and approval” work flow, see "Request and Approval Workflow Overview" on page 774.

   For more information about the “request and approval” work flow, see "Enabling Request and Approval Workflow" on page 475 and "Request and Approval Workflow Overview" on page 774."
6. Click **Show Password** to view the password for the selected account as plain text or click **Copy Password** to copy the password without viewing it.

   Depending on how authentication rules and authentication profiles are configured, you might be required to respond to one or more authentication challenges before viewing or copying the stored password. If you are able to authenticate successfully, the checkout proceeds.

   Password checkouts are recorded as recent activity in the dashboard, in your workspace, and in the list of system, domain, or database activity.
7. Click **Close**.

After you take the appropriate action on the remote computer, close the session to log off and check in the password. You can check in the password from any location where the account you have checked out is visible. For more information about checking in a password, see "Logging on Without a Password" on page 676.

Extending Password Checkout Time

If you have the appropriate administrative rights and you have checked out the password for a stored account, you can extend the checkout time to allow you to continue maintenance or perform administrative operations.

The default maximum length of time you are allowed to keep a password checked out is configured using a system, domain, database, or account policy. If the maximum checkout lifetime is 60 minutes and you extend the checkout time before time runs out, the password expiration is reset to 60 minutes.

You can extend the checkout time for a password indefinitely at any point in its lifetime as long as you extend the checkout time before the checkout period expires. For example, if you have extended the checkout time for 60 minutes, but need more time to resolve an issue, you can extend the checkout time for another 60 minutes as long as you do so before the first 60 minutes expires. For more information about configuring the Checkout lifetime policy, see "Setting System-specific Policies" on page 556.

To extend the check out time for a password:

1. Go to **Admin Portal** > **Resources** > **Accounts** to display the list of accounts.

   You can extend the check out time for a password from any list of accounts. For example, the action is available if you are viewing the list of accounts for any specific system, domain, or database.
2. Select an account.
3. Click the Actions menu, then click **Extend**.

After you are finished performing maintenance or administrative tasks, log off and check in the password. For more information about checking in a password, see "Logging on Without a Password" on page 676.

Checking in Passwords

After you check out a password, you have a limited period of time in which the password you checked out is valid for activity on a remote system, domain, or database. If the Privileged Access Service manages the password for the account, you should check in the password when you end the session on the remote system, so that a new secure password can be generated for the account you used.

To check in a password you have previously checked out:

1. In the Admin Portal, click **Resources**, then click **Accounts** to display the list of accounts.

   You can check in a password that you have previously checked out from any list of accounts. For example, the action is available if you are viewing the list of accounts for any specific system, domain, or database.
2. Select an account.
3. Click the Actions menu, then click **Check-in**.

Accessing Cloud Providers

To access the Cloud Providers page, navigate to **Resources** > **Cloud Providers**. Once there, you can add and update a cloud provider. For more information on adding a cloud provider, see "Managing a Cloud Provider Account" on page 567.

Accessing Databases

To access the accounts page, navigate to **Resources** > **Databases**. Once there, you can perform the following tasks:

- "Viewing the databases you've added"
- "Selecting a database"
- "Deleting a database"
- "Deleting a database account"
- "Modifying Database Sets" on page 669
- "Modifying Database-specific Details" on page 660

Checking in Passwords

After you check out a password, you have a limited period of time in which that password is valid for database activity. If Privileged Access Service manages the password for the account, you should check in the password when you end the database session, so that a new secure password can be generated for the account you used.

You can check in a password or multiple passwords you have previously checked out from the **Accounts** or **Workspace** tab. For example, if you are viewing the list of database accounts, you can select an account and click the Actions menu to check in a password that you currently have checked out.

To check in a password you have previously checked out:

1. Go to **Admin Portal** > **Resources** > **Databases** to display the list of databases.
2. Select a database to display the database details.
3. Select a database account or multiple accounts, then click the **Actions** menu.
4. Click **Check-in**.

You can also check in an account password when you are viewing your own activity on the **Workspace** tab. or when viewing accounts on the **Accounts** tab. For more information about reviewing the summary of your activity, see "Viewing Dashboards" on page 1069. For more information about working with accounts directly, see "Managing Accounts" on page 645.

Checking out Account Passwords

When you add database accounts to the Privileged Access Service, you can store the passwords for those accounts securely in a local repository, in the Delinea, or in a key management appliance such as SafeNet KeySecure. If you have the appropriate global or database-specific permissions, you can check out the password for a stored database account used to connect to a database. When you check out a password, you choose whether to display or copy it to the clipboard for use. The password remains checked out until either you check it back in or the Privileged Access Service checks it automatically.

The maximum length of time you are allowed to keep a password checked out is configured by the "Setting Database-specific Policies" on page 485 policy. However, you can extend the checkout time for a password that is currently checked out, if needed. For more information about configuring the Checkout lifetime policy, see "Setting Database-specific Policies" on page 485. For more information about extending the checkout time, see "Extending the password checkout time."

To check out a database account password:

1. In the Admin Portal go to **Resources > Databases** to display the list of databases.
2. Select a database to display the database details.
3. Select the appropriate database account from the list of accounts, then click **Checkout** or **Request Checkout**.

   If you don't have the Checkout permission and click Request Checkout, your request is sent to a designated user or to the members of a designated role for approval. If your request is approved, you have limited period of time to check out the account password. For more information about the "request and approval" work flow, see "Request and Approval Workflow Overview" on page 774.
4. Click **Show Password** if you want to view the password for the selected account as plain text or click **Copy Password** to copy the password without viewing it.

   Depending on how authentication rules and authentication profiles are configured for the database and account, you might be required to respond to one or more authentication challenges before viewing or copying the stored password. If you are able to authenticate successfully by responding to one or more authentication challenges, the checkout proceeds. The checkout is then recorded as recent activity in the dashboard, in your workspace, and in the list of database activity.
5. Click **Close**.
6. Log on to the database using the selected account name and password.

After taking the appropriate action on the database, close the session to log off and check in the password. For more information about checking in a password, see "Checking in a Password from the Workspace" on page 1052.

Extending Password Checkout Time

If you have the appropriate administrative rights and you have checked out the password for a saved database account name, you can extend the checkout time to allow you to continue maintenance or perform administrative operations. The default maximum length of time you are allowed to keep a password checked out is configured using "Checkout lifetime" policy. If the maximum checkout lifetime is 60 minutes and you extend the checkout time before time runs out, the password expiration is reset to 60 minutes.

You can extend the checkout time for a password indefinitely at any point in its lifetime as long as you extend the checkout time before the checkout period expires. For example, if you have extended the checkout time for 60 minutes, but need more time to resolve an issue, you can extend the checkout time for another 60 minutes as long as you do so before the first 60 minutes expires. For more information about configuring the Checkout lifetime policy, see "Setting Database-specific Policies" on page 485.

To extend the check out time for a password:

1. Go to **Admin Portal** > **Resources** > **Domains** to display the list of databases.
2. Select a database to display the database details.
3. Click **Accounts**, then right-click the account that is currently checked out.
4. Click **Extend**.

   After you extend the checkout time for a password, the activity is logged on the Privileged Access Service dashboard.

After you are finished performing maintenance or administrative tasks on the target database, log off, and check in the password. For more information about checking in a password, see "Checking in a Password from the Workspace" on page 1052.

Launching Desktop Apps from Databases

If you have desktop applications configured and the database is referenced in the **Command Line** field, then you will see the launch action for that application. See "Adding Desktop Apps Using the Admin Portal" on page 932 for information on configuring desktop applications.

To launch a desktop application:

1. Log in to Admin Portal.
2. Click **Resources** > **Databases** to display the list of databases.
3. Select a database to display its details.
4. Click the Actions menu, go to **Launch <desktop application name>** to launch the specified application.
5. Provide the relevant credentials if required.

Selecting Databases

You can select a database to work with by clicking anywhere in the row that contains the database name to display the database details or by clicking the check box for a row. Selecting a database displays the Actions menu. From the Actions menu, you can click:

- **Add to Set** to add the selected system to a new or existing set.
- **Delete** to remove a database from the list.
- **Test connection** to perform a check on the selected database and determine if the database is reachable. The Test connection function is not supported for the SQL Server database type if a port number is not specified.

You can also select an action from the Actions menu when viewing the details for an individual database or view and modify database-specific information. For example, when you are displaying the details for a selected database, you can do the following:

- Change database settings such as the database name and description.
- Add database accounts and view database account activity, such as the date and time of the last password reset and the number of active sessions for the account.
- Specify the connectors to use for the database.
- Set database-specific policies.
- View recent activity for the database, such as who has checked out or checked in a password for database accounts.
- Set database-specific permissions for the users who are allowed to access the database with stored accounts.

Accessing Desktop Apps

To access the accounts page, navigate to **Apps** > **Desktop Apps**. Once there, you can perform the following task:

Selecting Actions for Desktop Apps

Click anywhere in the row that contains the desktop app name to display application configuration details. Click the check box next to the application to view the available list of Actions for the application. The same actions are also available from the Actions menu when you click the desktop app. You can select the following actions:

Launch to log in to the desktop app with the configured credentials. For information on the available keyboard shortcuts, see "Using Default Web-based Clients" on page 711.

Add To Set to add the selected desktop app to a new or existing set. Also see "Adding Desktop App Sets" on page 932 and "Managing application sets."

Delete to remove a desktop app from the list. You cannot delete desktop apps that have an active session.

After you have added desktop apps, you can organize them into logical groups—desktop app sets—to simplify management activity and reporting for attributes in common.

Accessing Domains

To access the accounts page, navigate to **Resources** > **Domains**. Once there, you can perform the following task:

Logging on Domain Computers

When you add domain accounts to the Privileged Access Service, you can store the passwords for those accounts securely in a local repository, in the Delinea service, or in a key management appliance such as SafeNet KeySecure. If you have the appropriate global- or domain-specific permissions, you can then use the account and its stored password to log on to any domain computers that the account has permission to access. The permissions for the Active Directory accounts you can use to log on are controlled through access control lists (ACL). By storing these accounts in the Privileged Access Service, you can make the account available to multiple users without sharing the password.

To log on to a domain computer:

1. In the Admin Portal, click **Resources > Domains** to display the list of domains.
2. Select the domain computer in the list of systems and open the Actions menu.
3. Click **Select/Request Account**.
4. Type a search string to filter the list of accounts.
5. Select the Active Directory account you want to use to log on to the domain computer, then click **Select**.

   If the selected account has permission to access the selected domain computer, a remote desktop connection starts a new session on the computer for you to perform whatever tasks are required using the Active Directory account you selected.

For information about adding domain computers as systems, see "Adding Windows Systems" on page 545 in "Managing Systems" on page 687.

Accessing Secrets

To access the accounts page, navigate to **Resources** > **Secrets**. Once there, you can perform the following tasks:

- "Retrieving a secret"
- "Launching a desktop application from secret"

Launching Desktop Apps from Secrets

If you have desktop applications configured and the secret is referenced in the **Command Line** field, then you will see the launch action for that application. See "Adding Desktop Apps Using the Admin Portal" on page 932 for information on configuring desktop applications.

To launch a desktop application:

1. Log in to Admin Portal,
2. Click **Resources > Secrets** to display the list of secrets.
3. Select a secret to display its details.
4. Click the Actions menu > **Launch <desktop application name>** to launch the specified application.
5. Provide the relevant credentials if required.

Retrieving Secrets

If you are the owner of a secret text string or stored file, you can view or download the secrets you own. If you are in a role with the appropriate administrative rights and have been granted the Retrieve Secret permission, or the secret is located in a folder that grants you the Retrieve Secret permission, you can view or download secrets.

There are different ways to navigate to the Retrieve action. After you select this action, however, the steps are similar.

To retrieve a secret:

1. In the Admin Portal, click **Resources**, then click **Secrets** to display the list of secrets.
2. Select a secret to display its details.
3. Click the **Actions** menu, then click **Retrieve**.
   - If the secret is a text string, you can display or copy the text, then close or cancel the retrieval options box.
   - If the secret is a stored file that is not protected by a password, you can click the file name to download it.
   - If the secret is a stored file that is protected by a password, you can show or copy the password so that you can provide this information where required. You can then click the file name to download the file.

   You should note that if you store an optional password with a secret file, that password is not used to retrieve the file. The password and the file are simply stored together for your convenience. You might be prompted to provide the password when you attempt to open the file after downloading it.

Accessing Systems

You can access any system you have added to Privileged Access Service (displayed in **Admin Portal > Resources > Systems**) by clicking anywhere in the row that contains the system name or clicking the checkbox next to the system name. Once you have selected the system you can select actions from system details or select available Actions from the Actions drop down menu.

See the following for additional information:

- "Selecting actions for a system"
- "Logging on Without a Password" on page 676
- "Logging on manually"
- "Connecting to target systems"
- "Connecting to Network Systems" below

Connecting to Network Systems

With the Privileged Access Service, you can securely store local user name and password combinations (accounts). You can then use those accounts to connect interactively to servers, switches, and routers (systems). You can also choose who is authorized to use the accounts on which systems and who is authorized to view or copy the account password.

The systems you manage might include servers and network devices inside of your organization's firewall, outside of the firewall, or a combination of the two. For example, you might have some users who can log on to specific systems inside of the firewall and others who can access specific systems located outside of the firewall.

In the most common scenario, you would add shared local accounts—such as root, patrol, or oracle—for the systems you add to the Privileged Access Service. You would also specify which users are allowed to use those shared accounts and what different users are allowed to do. For example, you can specify which users can connect using a given account without having to specify the password for the account.

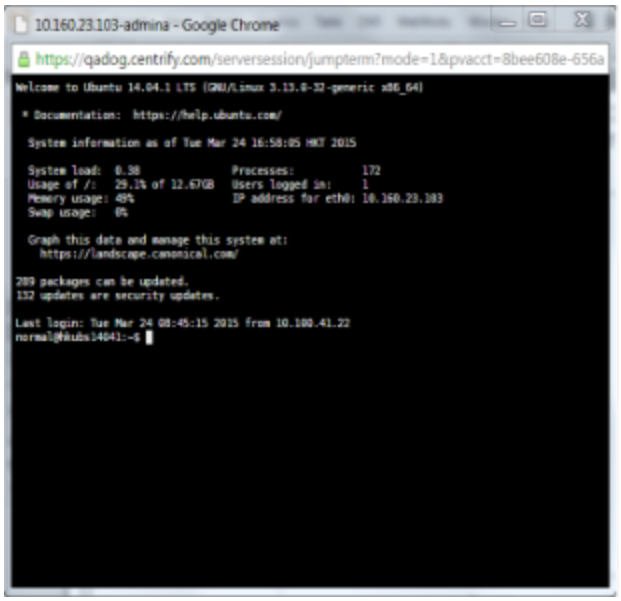
Connecting Systems

You must have the RDP or SSH gateway service enabled for at least one connector to log on remotely to target systems using RDP or SSH. If the gateway service is available for a connector in your infrastructure and you have appropriate permissions, you can log on either by using stored account information or by manually specifying a user name and password.

You can also configure remote connections to use a local Windows client or native UNIX SSH client instead of the default web-based client. These connections also require the SSH gateway service to be enabled on an available connector to log on to the target system.

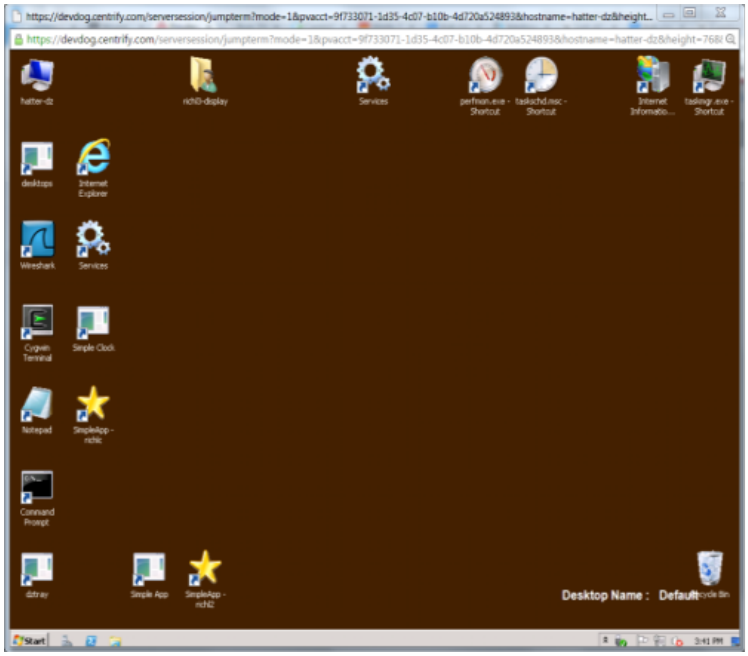
Linux and UNIX Target Systems

If the target system is a UNIX server or a network device that supports SSH, logging on opens a new web-based client SSH session by default. For example, a session window might look similar to this:



Windows Target Systems

If the target system is a Windows computer, logging on opens a new web-based client remote desktop connection. For example, a remote desktop session window might look similar to this:

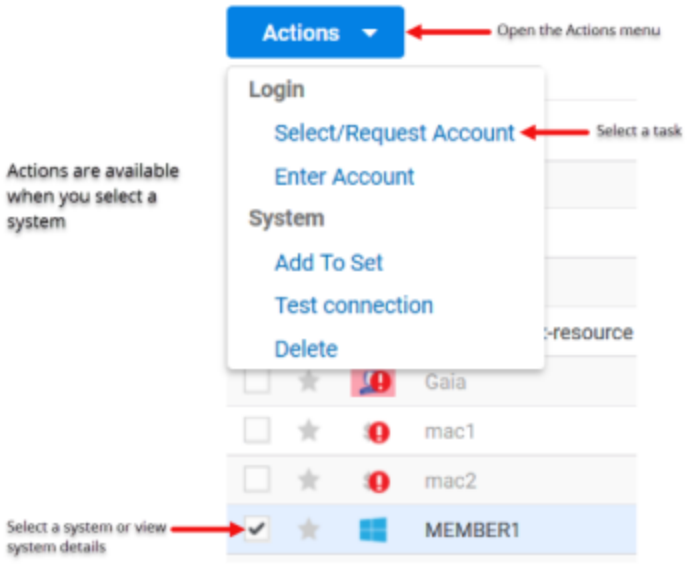


For more information about interacting with a target system after logging on using the default web-based browser client, see "Using Default Web-based Clients" on page 711. For information about adding the RDP or SSH gateway service to a connector, see "Selecting Connector Services" on page 700. For information about selecting the remote client program you want to use for connecting to target systems, see "Accessing Remote Systems" on page 701.

Selecting System Actions

You can select a system to work with by clicking anywhere in the row that contains the system name to display the system details or by clicking the check box for a row. Selecting a system displays the Actions menu from which you can select the action you want to perform.

For example, select a system using the check box, then click Actions to display the list of potential actions.



The same actions are available from the Actions menu when you view the details for an individual system. For most systems, you can select the following actions:

- **Select/Request Account** to search for and select the account you want to use to log on to the system.
- **Enter Account** to log on by specifying a user name and password.
- **Add to Set** to add the selected system to a new or existing set.
- **Test connection** to perform a health check on the selected system and determine if the system is reachable.
- **Delete** to remove a system from the list.

Most of the actions you can select perform a task directly on the selected system. For example, you can open a remote session on the system using the password for an account you select or using a specified user name and password. The permissions associated with your account determine which tasks you can perform, however. For example, if you don't have the Login permission but a request and approval work flow is enabled, you might be able to submit a request to a designated approver to log on to a selected system.

For more information about configuring, requesting, and responding to access requests, see "Request and Approval Workflow Overview" on page 774. Also see [Management port for password operations."

Depending on the system you have selected, you might also see the **Use My Account** action. This action can only be executed on computers where additional configuration steps have been performed. For more information about how to configure a computer to use this action, see "Authenticating with a single-use SSH Certificate."

If you have desktop applications configured and the system is referenced in the **Command Line** field, then you will see the launch action for that application. See "Adding Desktop Apps Using the Admin Portal" on page 932 for information on configuring desktop applications.

Logging on without Passwords

After you add account information to the Privileged Access Service, other users with the appropriate global- or system-specific permission can log on using the account without knowing the password for the account.

When you select an account stored in the Privileged Access Service to log on to a target system, the Privileged Access Service opens a secure shell connection if the target system is a UNIX, Generic SSH, or supported network system or a remote desktop connection if the target system is a Windows computer. If the target system does not use the default port for secure shell or remote desktop connections, you can specify the port to use by clicking System Settings for a selected system. For more information about changing settings for a target system, see "Changing System Settings" on page 687.

To log on using saved account information:

1. In the Admin Portal, click **Resources**, then click **Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Click the Actions menu, then select **Select/Request Account**.
4. Type a string to search for and select the appropriate account from the list of stored accounts, then click **Select**.

   Some organizations may have their tenant configured so that the list of domain accounts doesn't automatically load; enabling this configuration can help with performance if you have a substantial number of accounts. If you have this configuration enabled:

   - You can also filter your search by domains and child domains listed under the Domains section of the search filter. Use the arrow to expand or collapse the domain groups.
   - To use domain accounts, check the domain(s) you want to use for your filter, then type in the search box. The search will return results matching your search term from domain accounts as well as local accounts.

If you have the Login permission and the stored credentials are valid, a new interactive secure shell or remote desktop session opens on the target system. Within the secure shell or remote desktop session, most operations—such as cut and paste or resizing of windows—work as you would expect them to. For more information about working in the remote session, see "Connecting to target systems."

If a “request and approval” work flow is enabled, your account access request is sent to a designated user or to the members of a designated role for approval. If your request is approved, you have limited period of time to start a new interactive secure shell or remote desktop session on the target system. For more information about the “request and approval” work flow, see "Managing Domains" on page 671.

Depending on how authentication rules and authentication profiles are configured for the system and account, you might be required to respond to one or more authentication challenges before logging on to the remote system. If you are able to authenticate successfully by responding to the authentication challenges, the session opens and the activity is recorded in the dashboard and in the list of system activity.

Manual Logon

You can also log on to any target system you add to the Privileged Access Service without using any account information that's stored in the Privileged Access Service. You can use any valid credentials to log on manually to a target system.

To log on by specifying a user name and password:

1. In the Admin Portal, click **Resources**, then click **Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Click the Actions menu, then click **Enter Account**.
4. Type the user name and password and click **Login**.

   Depending on how authentication rules and authentication profiles are configured for the system and account, you might be required to respond to an additional authentication challenges before logging on.

If the credentials you specify are valid for the target system, logging on starts a new interactive secure shell or remote desktop session on the target system. Within the secure shell or remote desktop session, most operations—such as cut and paste or resizing of windows—work as you would expect them to. For more information about working in the remote session, see "Connecting to target systems."

Successful and failed login attempts and active sessions are recorded as recent activity in the dashboard, in your workspace, and in the list of system activity.

Checking out Managed Account Passwords

If you are authorized to check out passwords, you can retrieve the password for an account to enable you to log on to a target system. After you retrieve the password, it can remain checked out for a configurable period of time. What happens at the end of the allowed checkout period depends on whether the account password is managed by the Privileged Access Service or unmanaged.

If the password is a managed account password:

- The password you retrieved expires at the end of the checkout period and Privileged Access Service automatically generates a new password for the account.
- If you check in the password before the end of the checkout period, the check in process also automatically generates a new password for the account.
- After each password rotation, users can check out the new password.

  Note: The password rotation ends existing password checkouts. This means any password checkouts will be checked back in.

- You can use policies to configure the maximum number of minutes a password can be checked out and whether multiple administrators can have a password checked out at the same time.

  Note: If **Workflow** is enabled on the user's account, and the user requests permission using **Request Checkout**, the password can only be checked out during the time period specified by the admin. For example between 1pm - 2pm. This adjusts the checkout duration to ensure the password is checked back in by the end of the time period. For example 2pm.

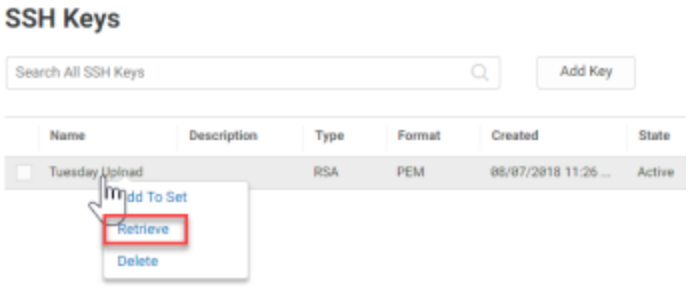
- You can also extend the password checkout time for a currently checked out password if you need more time to complete your work. With a managed account password, however, the only valid password is the one known and updated by the Privileged Access Service.

Retrieving SSH Keys

You can retrieve a public or private SSH key. Typically, you retrieve a public key when you need access to a new system and your SSH client already has a private key configured on it. You typically retrieve a private key when you need to access a system that already has a public key configured, but your SSH client does not have a private key configured on it. To retrieve a key from Admin Portal, you must have first added it to Privileged Access Service. See "Adding SSH keys" on page 512 for instructions.

To retrieve a SSH key:

1. Click **Resources** > **SSH Keys**.
2. Right-click the relevant key and select **Retrieve**.



3.
4. The Retrieve SSH Key window opens.
5. a. Select either Public Key or Private Key.
   b. Select the **Key Type** that you want to retrieve.
   c. This option is only available for public key retrieval. Private key retrieval supports only the PEM format.
   d. Click either the **Download Key** or **Copy Key** button.
   e. **Download Key** downloads the key to your default download folder.
   f. **Copy Key** allows you to paste the key to Notepad, MS Word, or other text-based software.
   g. (Optional) Enter the passphrase you would like to associate with the SSH key. Without a passphrase, the SSH Key is unencrypted by default.
   h. Click **Close**.

Adding Attributes for Systems and Accounts

System administrators can create and configure custom attributes for systems and accounts. In addition, any user with edit permissions on a system or account can set or modify the attribute values.

Note: You can also create and modify additional attributes using the API.

To create a custom attribute:

Note: Only system administrators can create a custom attribute

1. In the Admin Portal, navigate to **Settings** > **Resources** > **Additional attributes**.
2. Depending on where you want to add your attribute, choose the **Systems** or **Accounts** tab.
3. Click **Add**.
4. Fill in the attribute information.

   Note: The attribute name must contain an underscore. This prevents name conflicts with the existing built-in attributes.

To view or modify attribute values for a system or account:

1. In the Admin Portal, navigate to **Resources** > **Systems**.
2. Click the system that contains your attribute.
3. Click **Additional Attributes** to see a list of the system's additional attributes.
4. To change a system attribute value, click the icon next to the existing attribute value to bring up the edit mode, change the value and click **Save**.
5. Click the **Accounts** tab and choose the account that contains your account attribute.
6. Click **Additional Attributes** to see a list of the account's additional attributes.
7. To change an account attribute value, click the icon next to the existing attribute value and click **Save**.

To view your attribute values in the data dictionary:

1. In the Admin Portal, navigate to **Reports**.
2. The attributes appear in the Data Dictionary list under the following tables :
   a. Server
   b. Vault Account

Adding Resources

You can add resources (systems, databases, domains, accounts, secrets, SSH keys, and services) to the Admin Portal and manage access to those resources.

For most systems that you add, you can log on and perform remote operations through secure shell (SSH) or remote desktop (RDP) sessions.

Adding Accounts

The Accounts page in **Resources > Accounts** displays the list of accounts initially added when you added resources (systems, domains, and databases) to the Privileged Access Service. If you did not add an account when you added or imported resources, provided invalid account information, or want to update the resource to include additional accounts, you can do so by clicking Accounts when viewing the details for a particular resource.

Note: To add an account(s), enable the "Add Account" permission for all users including System Administrators. Additionally, you must add the user to the Administrator role.

For additional information, see the following topics:

- "Using Managed or Unmanaged Accounts" on page 477
- "Storing Accounts for Domains and Databases" on page 477
- "Adding Account Sets" below
- "Setting Account Permissions" on the next page
- "Setting Password Checkout Policy" on page 477
- "Enabling Request and Approval Workflow" below

Adding Account Sets

After you have added accounts for systems, domains, or databases, you can organize them into logical groups—account sets—to simplify management activity and reporting for accounts with attributes in common.

You cannot add multiplexed accounts to an account set.

To add an account set:

1. In the Admin Portal, click **Resources**, then click **Accounts** to display the list of accounts.
2. In the Sets section, click **Add** to create a new set.
3. Type a name for the new set, an optional description, and select whether group membership is manual or dynamic.

   For manual sets, you can specify permissions for both the set itself and the members of the set. For dynamic sets, you can only specify permissions on the set.
4. Identify the members of the set in one of two ways.
   - If set membership is Dynamic, type the SQL statement to execute to identify set members in the Query field. For example, if you want to add a set for the accounts with an account name of root, you could type a SQL statement like this:

     select id from VaultAccount where name like 'root'
   - If you select **Manual**, click **Members**, then click **Add** to search for and select the databases to add as members.
5. Click **Save**.

Enabling Request and Approval Workflow

You can enable a “request and approval” workflow for specific accounts stored in the Privileged Access Service. Users who don’t have access by default can then submit requests to a designated approver who has the authority to grant or deny them access. By enabling a workflow, users can request access to the privileged accounts you specify and, if their request is approved, check out the account password or use the account to log on remotely.

You can also explicitly prevent an account from being available for access requests. For example, you might configure a “request and approval” workflow for all accounts, then identify a few accounts which do not allow access requests.

To enable workflow for a specific account:

1. In the Admin Portal, click **Resources**, then click **Accounts** to display the list of accounts.
2. Click Local Accounts, Domain Accounts, or Database Accounts to select the type of account you want to modify.
3. From the list of local, domain, or database accounts, select the specific account for which you want to enable workflow.
4. From the account details, click **Workflow**.
5. Select **Yes**.
6. Search for and select an appropriate user, group, or role to approve requests, then click **Add**.
7. Click **Save**.

For more information about configuring a “request and approval” workflow, requesting access, and approving requests, see "Request and Approval Workflow Overview" on page 774.

Setting Account Permissions

If you are viewing the account details, you can click Permissions to specify the individual users, groups, roles, or computers that are allowed to use the account and what each user, group, role, or computer has permission to do when using the account.

To set permissions for an account:

1. In the Admin Portal, click **Resources**, then click **Accounts** to display the list of accounts.
2. Click Local Accounts, Domain Accounts, Database Accounts, or Multiplexed Accounts to select the type of account to which you want to grant access.
3. Select the specific account to which you want to grant access to display the account details.
4. Click Permissions, then click **Add**.
5. Type all or part of the user, group, role, or computer name you want to find.
6. Select the appropriate users, groups, roles, or computers from the search results, then click Add.

   For example, if you have added the account root-1 for a target system, you might want to add the onsite-IT@pubs.org role and the offshore-IT@pubs.org role to specify what members of each role can do when using the root-1 account.
7. Select the appropriate permissions for each user, group, role, or computer you have added, then click **Save**.

   For example, you might want to give the members of the onsite-IT@pubs.org role permission to perform all tasks using the root account but only assign the View and Edit permissions to the members of the offshore-IT@pubs.org role.

You must select at least one permission for the user, group, or role before you can save changes to the account.

As a system administrator, your user account has full permissions by default. The Grant permission enables you to assign permissions to other users on an account-by-account basis or globally to control which actions are available for different users.

For more information about setting permissions for other users, see "Assigning Permissions" on page 743. For information about assigning global account permissions, see "Setting Global Account Permissions" on page 750.

Setting Password Checkout Policy

You can configure authentication rules and authentication profiles to protect access to the account password for specific accounts. Based on the rules you define, users attempting to check out the password for an account with access to a specific system might be required to provide a password, enter the passcode from a text message, or answer a phone call to authentication their identity. The authentication rule defines the conditions for when a specific authentication profile should be used. The authentication profile defines the types of challenges presented and whether one factor or two factor authentication is required. You can also define a default authentication profile to use if the conditions you specify for the checkout rules are not met.

If you don't create any authentication rules or authentication profiles for password checkouts, users with the appropriate permission can check out stored account passwords without being challenged to re-authenticate their identity or provide multi-factor authentication.

For more information about setting the password checkout policy, see the following topics:

- "Supported Authentication Challenges" on page 558
- "Authenticating If Managing Services On-Site" on page 558

Storing Accounts for Domains and Databases

In addition to local accounts such as root for Linux or UNIX or Administrator for Windows, you can use the Privileged Access Service to store account information for domains and databases. By storing this information in the Privileged Access Service, you can control who can check out account passwords and automatically rotate the password for the privileged accounts you want to manage.

Using Managed or Unmanaged Accounts

If you use secure shell or remote desktop connections for a system, the account used to connect to the system can be either a **managed account**, that is, an account with the password automatically changed by the Privileged Access Service, or an **unmanaged account** with a password that is stored by the Privileged Access Service but not changed. In either case, the Privileged Access Service can retrieve the password programmatically without revealing it, so that administrators can use the account without knowing the password being used.

By logging on to target systems without a password, you can keep shared accounts more secure and enable administrators to open sessions from within or outside of the firewall based on how you choose to deploy the service.

Adding Databases

If you want to manage accounts for database services through the Privileged Access Service, you must first add the database to the Databases list. Initially, you might add databases and accounts one-by-one using the Add Database Wizard, which guides you through the information required. Alternatively, you can create an import file to add multiple databases and database accounts at once.

To add a new database to the database list

1. In the Admin Portal, click **Resources**, then click **Databases** to display the list of databases.
2. Click **Add Database** to open the Add Database Wizard.

3. Type a unique name to identify the database, select the type of database service you are adding, and specify the fully-qualified DNS host name or IP address, and click **Next**.
   - If the database type is **SQL Server**, you should also specify an instance name unless you are using the default instance rather than a named instance and the server must use Mixed authentication and the accounts you add must be SQL Server login accounts and use SQL Server authentication.
   - Note the following configuration instance that could cause a failed connection. If the SQL Server database is on a named instance or on the default instance but not using default 1433 port, then the connection will fail even if the port is not specified and the SQL Server Browser service is not running.
   - If the SQL Server database to be connected is the default instance (i.e. instance is not specified), even if the port is not specified and the SQL Server Browser service is not running, the SQL Server database server would try to connect to the database using the default port (i.e. 1433) and the database connection would be successful.
   - If the database type is **Oracle**, you must also specify a database service name and the accounts you add must be Oracle database accounts.
   - If the database type is **SAP ASE**, the accounts you add must be Adaptive Server Enterprise (ASE) database accounts.

   Optionally, you can also type a longer description for the database. For example, you might want to make note of the applications the database supports or the physical location of the server, then click Next to continue.
4. (SAP ASE Databases only) Either upload your SSL certificate now or add the certificate later by going to the **Settings** pane for this database. Upload the certificate or add it manually.
   - Select **Use SSL Certificate**, and either click **Upload File** to upload your certificate or click **Manual** and then click **Enter Key** to paste your certificate.
5. Add a user name and password for an account used to access the database and specify whether the password for the account is managed by the Privileged Access Service, then click **Next**.
6. Select **Verify Database Settings** to test access to the database using the account information provided, then click **Finish**.

   If the database and account settings are successfully verified, click **Close**.

   If there's an error, test network connectivity and verify that the user name and password you provided are valid for the database you are attempting to add. If verification fails, close the error message, deselect the **Verify Database Settings** option, then click **Finish** to add the database and close the **Add Database Wizard**. You can only deselect the Verify Database Settings option if the password for the account is unmanaged. If the password for an account is managed, the database account must be verified to ensure the correct password is stored by the Privileged Access Service.

Adding Database Sets

After you have added databases, you can organize them into logical groups—database sets—to simplify management activity and reporting for databases with attributes in common.

To add a database set:

1. In the Admin Portal, click **Resources**, then click **Databases** to display the list of databases.
2. In the Sets section, click **Add** to create a new set.
3. Type a name for the new set, an optional description, and select whether group membership is manual or dynamic.

   For manual sets, you can specify permissions for both the set itself and the members of the set. For dynamic sets, you can only specify permissions on the set.
4. Identify the members of the set in one of two ways.
   - If set membership is Dynamic, type the SQL statement to execute to identify set members in the Query field. For example, if you want to add a set for the databases with a name that starts with ora, you could type a SQL statement like this:

     ```
     select id from VaultDatabase where name like 'ora%'
     ```

   - If you select **Manual**, click **Members**, then click **Add** to search for and select the databases to add as members.
5. Click **Save**.

Planning for Adding Database Accounts

Before adding any databases to the Privileged Access Service, you might want to consider which accounts you need to manage and whether there are any restrictions on those accounts that you should be aware of.

The most common accounts that are likely candidates to be managed through the Privileged Access Service include the system administrator accounts such as the sa account for Microsoft SQL Server databases, the SYSTEM administrative account for Oracle databases, the DBA administrative account for SAP Adaptive Server Enterprise databases, or any other account you use for database administration.

You might have many other administrative or in-house database accounts that require special privileges or have access to sensitive information. You can use Privileged Access Service to manage the password for any of these accounts or add non-administrative accounts to securely store the account information without having the password managed by Privileged Access Service.

Note: For supported infrastructure (for example: systems and databases), account names are often case sensitive. Ensure the account entered in Privileged Access Service matches the account in the infrastructure.

For more information about the requirements for adding databases and database account, see the following topics:

Requirements for Microsoft SQL Server Databases

Before attempting to add Microsoft SQL Server database accounts to the Privileged Access Service, you should keep the following requirements in mind:

- You can only use the Privileged Access Service to manage passwords for local SQL Server Login database accounts that use SQL Server authentication.
- You cannot rotate or manage expired passwords for managed accounts.

- If you are using Windows authentication to connect to the SQL Server database, you should add domain accounts to the Privileged Access Service to manage those accounts.

Database Accounts and Clustering

The accounts used to communicate with databases fall into two major categories: **administrative accounts** and **service accounts**. Administrative accounts are used by the database administrator to connect to the database to perform administrative tasks, such as adding new databases or database users or managing database tables. Service accounts are used by application servers—such as Tomcat, JBoss, or IIS—to authenticate to the database before storing or retrieving service-specific information in the database. The Privileged Access Service supports password management for the administrative database accounts.

In addition, there are two types of authentication for database accounts in SQL Server:

- Windows authentication
- SQL Server authentication

You can use the Privileged Access Service to manage the password for both Windows authentication database accounts and SQL Server authentication database accounts for standalone SQL Server instances.

If you have a SQL Server cluster configured for high availability using automatic failover, the administrative database accounts you manage should be domain accounts that use Windows authentication domain to avoid the replication issues.

If the managed database account is a Windows domain account, passwords can be synchronized for SQL Server clusters that are configured to use failover clustered instances, database mirroring, AlwaysOn availability groups, log shipping, or any combination of these features.

If you use SQL Server authentication for the database account you want to manage, the SQL Server cluster must be configured to use failover clustered instances. For managed SQL Server database accounts, only failover clustered instances are supported because other high-availability features might result in replication delays and authentication failures.

For details about the versions of Microsoft SQL Server supported in the current release, see the release notes. For information about configuring clustering for SQL Server and clustering scenarios, see the Microsoft documentation.

Requirements for Oracle Database Accounts

Before attempting to add Oracle database accounts to the Privileged Access Service, you should keep the following requirements in mind:

You can only use the Privileged Access Service to manage passwords for local Oracle database accounts.

The accounts you manage must be configured to include the CREATE SESSION privilege.

You cannot rotate or manage expired passwords for managed accounts.

You cannot use the Privileged Access Service to manage the password for the SYS account because that account requires a physical password file. If you attempt to manage the password for the SYS account, you will see an “Invalid account credentials” error.

The computer where the connector is installed must have the Oracle Data Provider for the .NET Managed Driver (ODP.NET) client library installed in the global assembly catalog. You can download the latest Oracle ODP.NETmanaged driver and Install the ODP.NET client library. If you download and install the library after you

install the Delinea Connector, you should restart the connector before adding the database to Privileged Access Service.

Privileged Access Service can manage the account password for standalone Oracle server, or synchronize managed passwords across computers in a Real Application Cluster (RAC).

Oracle Database Support

The following Oracle databases are supported: 11g, 12c, 18c , and 19c. For more details about which versions of the Oracle database are supported in the current release, see the release notes.

Oracle databases can be configured to allow encrypted connections from the Connector.

Configuring Oracle Real-Application Clusters (RAC)

When configuring the Privileged Access Service for the databases in an Oracle Real Application Cluster, use the following settings:

Service Type: Oracle

Hostname: SCAN name

Port: SCAN port

Service Name: global Database Name

The SCAN name and port can be found with the following sqlplus command:

```
show parameter remote_listener
```

The global Database Name can be found with the following sqlplus command:

```
select * from global_NAME
```

Configure Oracle Data Guard

This section describes how to set the DNS alias when configuring the Oracle Data Guard.

To set the DNS alias:

1. Login the DNS Server Administrator.
2. Open **DNS Manager**.
3. Go to **Forward Lookup Zones**.
4. Right-click the target domain and choose **New Alias (CNAME)**.
5. Set an alias.
6. Input the target FQDN and click **OK**.
7. On the machine running the application, open the Command Prompt window as Administrator and enter the command:

8. run "ipconfig /flushdns"
9. Ping the alias in FQDN to check the target IP address.

Installing the ODP.NET client library

Before you install, ensure you download the "64-bit ODAC 19.3 installation package."

To install the ODP.NET client library:

1. Unzip the 64-bit ODAC 19.3 zip file.
2. Launch the Command Prompt using **Run as administrator**.
3. Use cd to navigate to the folder containing the unzipped files.
4. Run the command install.bat odp.net4 c:\oracle odac. This will install both the x86 and x64 drivers to the path c:\oracle.
5. To configure ODP.NET in GAC, use the Command Prompt to navigate to C:\oracle\odp.net\managed\x64 and run the following commands:

   OraProvCfg /action:config /product:odpm /frameworkversion:v4.0.30319 /providerpath:"C:\oracle\odp.net\managed\common\Oracle.ManagedDataAccess.dll" /set:settings\TNS_ADMIN:"C:\oracle\network\admin"

   OraProvCfg /action:gac /providerpath:"C:\oracle\odp.net\managed\common\Oracle.ManagedDataAccess.dll"

   OraProvCfg /action:gac /providerpath:"C:\oracle\odp.net\PublisherPolicy\4\Policy.4.122.Oracle.DataAccess.dll"
6. After the installation completes, restart the connector. This will ensure ODP.NET is correctly loaded.

Requirements for SAP Adaptive Server Enterprise

Before attempting to add SAP Adaptive Server Enterprise (ASE) database accounts to the Privileged Access Service, you should keep the following requirements in mind:

- You can only use the Privileged Access Service to manage passwords for local database accounts.
- You cannot rotate or manage expired passwords for managed accounts.
- Supported releases are subject to change based on the end of mainstream maintenance date as determined by SAP. For more details about which versions of the SAP ASE database are supported in the current release, see the release notes.
- The computer where the Delinea Connector is installed must have the SAP ASE Data Provider for the .NET client (ADO.NET) installed in the global assembly cache (GAC). For installation details, see "Installing ADO.NET with the Delinea Connector." If you download and install the library after you install the Delinea Connector, you should restart the connector before adding the database to Privileged Access Service. If you have an older version of the ADO.NET client library, check the SAP ASE website to see if a newer version is available.
- Privileged Access Service can manage the account password for a standalone SAP ASE servers, or synchronize managed passwords across computers in a Windows cluster.

- Support for password encryption is enabled in the Privileged Access Service SAP ASE plug in. If the SAP ASE server also has password encryption enabled, the password is encrypted before being sent to the server. For additional information on password encryption, see the SAP documentation.

Installing ADO.NET with the Delinea Connector

You must install the SAP ASE Data Provider for the .NET client (ADO.NET) on the computer where the Delinea Connector is installed.

To install ADO.NET Data Provider

1. On the computer where the Delinea Connector is installed, download SDK For SAP ASE 16.0 (Platform: Windows x64).

   If you do not have the SDK for SAP ASE 16.0, check the SAP support portal > Software Downloads or contact your SAP support representative.
2. Execute setup.exe.
3. In the installation menu, select **Customize installation. Select SAP ASE ADO.NET Data Provider.**
4. After installation, the Data Provider should be registered in the GAC.

   If it is not registered in the GAC, see SAP KB article 2139582 for additional information.

   https://apps.support.sap.com/sap/support/knowledge/preview/en/2139582

Configuring a DNS Alias for SAP ASE Failover Clusters

This section describes how to set the DNS alias when configuring an SAP ASE failover cluster. The configuration requires a DNS alias to map to the primary and secondary node IP address.

Note: You can install the SAP ASE database on a Windows Server but use another Linux server for DNS.

To set the DNS alias on a Windows Server:

1. Log in to the DNS Server Administrator.
2. Open the DNS Manager.
3. Go to Forward Lookup Zones.
4. Right-click the target domain and choose New Alias (CNAME).
5. Set an alias.
6. Input the target FQDN and click OK.
7. On the machine running the application, open the Command Prompt window as Administrator and enter the command:

   ```
   run "ipconfig /flushdns"
   ```
8. Ping the alias in FQDN to check the target IP address.

Setting Database-specific Advanced Options

You can set advanced security and maintenance settings for individual databases or database sets. You can also set security and maintenance options globally to apply to all databases except where you have explicitly defined a

database-specific setting. If you use a combination of global and database-specific settings, the database-specific settings take precedence over the global settings.

If you are not using global security settings or want to override global settings on specific databases, you can set the following advanced security and maintenance options on a case-by-case basis:

- "Allow multiple password checkouts"
- "Enable periodic password rotation"
- "Enable password rotation after check-in"
- "Minimum password age"
- "Password complexity profile"
- "Enable periodic password history cleanup"

To set database-specific advanced options:

1. In the Admin Portal, click **Resources**, then click **Databases** to display the list of databases.
2. Select the database to display the database-specific details.
3. Click **Advanced**.
4. Select settings for any or all of the advanced database options.
5. Click **Save**.

For more information about how to set the database-specific options, click the information icon in the Admin Portal.

Allowing Multiple-Password Checkouts

- Select **No** if only one administrator is allowed check out the password for a selected database account at any given time. If you select No, the administrator must check the password in and have a new password generated before another administrator can access the database with the updated password.
- Select **Yes** if you want to allow multiple users to have the database account password checked out at the same time for a selected database. If you select Yes, multiple administrators can check out the password for the database without waiting for the account password to be checked in.

Enabling Periodic Password Rotation

- Select **Yes** if you want to rotate managed passwords automatically at the interval you specify.
- Select **No** if you want to prevent password rotation for the selected database.
- If you select **Yes**, you should also specify the **Password rotation interval** in days. Type the maximum number of days to allow between automated password changes for managed accounts. You can set this policy to comply with your organization's password expiration policies. For example, your organization might require passwords to be changed every 90 days. You can use this policy to automatically update managed passwords at a maximum of every 90 days. If the policy is not defined, passwords are not rotated.

Enabling Password Rotation after Check-in

After you check out a managed password for a database, you can specify whether the managed password is rotated after it is checked in.

Select **Yes** to allow password rotation after password check in. Select **No** to not allow password rotation after it is checked in. Select ***--*** to use the default setting from the Security Settings in the Settings tab.

Minimum Password Age

Specify the minimum number of days that a managed password must have been in use before it can be rotated.

Password Complexity Profile

Select an existing password generation profile or add a new profile for the selected database. If you don't select or add a profile, the default password generation profile for the database type is used. For more information about adding and editing password complexity profiles, see "Configuring password profiles."

Enabling Periodic Password History Cleanup

- Select **Yes** to automatically delete retired passwords from the password history after a given number of days.
- Select **No** to prevent the from automatically deleting retired passwords from the password history at a set interval.
- If you select yes, you can also specify the maximum number of days of password history to keep. For example, if you have a requirement to keep a record of passwords used for three years, you might set the cleanup interval to 1096 days to maintain the password history for that period of time. If you select the default setting, retired passwords are automatically deleted after 365 days. You cannot set a cleanup interval less than 90 days.

Setting Database-specific Policies

Setting Policies

You can set the following policy for individual databases or database sets:

To set database-specific policies:

1. In the **Admin Portal > *Resources* > Databases** to display the list of databases.
2. Select the database to display the database-specific details.
3. Click **Policy**.
4. Select settings for any or all of the database policies.
5. Click **Save**.

For more information about how to set the databases-specific policies, click the policy link or the information icon in the Admin Portal. If you set polices globally, the global policies apply by default to all database accounts except where you have explicitly defined a database-specific policy.

Checkout Lifetime

Type the maximum number of minutes administrators are allowed to have a database account password checked out. After the number of minutes specified, the Privileged Access Service automatically checks the password back in. The minimum checkout lifetime is 15 minutes. If the policy is not defined, the default checkout lifetime is 60 minutes.

You can extend the checkout time for a password as long as you do so before the initial checkout period expires. For example, if the maximum checkout lifetime is 60 minutes and you extend the checkout time before the 60 minute period is over, the password expiration is reset to the 60 minute checkout lifetime. For more information about configuring the Checkout lifetime policy, see "Extending the password checkout time."

Adding Domains

Before you can store and manage passwords for Active Directory domain accounts, you must add the appropriate domains to the Privileged Access Service.

After you add the domains you want to manage, you can organize them into **domain sets** to simplify other tasks such as assigning set-specific permissions.

To add a new domain:

1. In the Admin Portal, click **Resources> Domains** to display the list of domains.
2. Click **Add Domain**.
3. Type the domain name and, optionally, a description to identify the domain.
4. Select Verify Domain to test access to the domain, then click Add. To verify access to the domain, at least one of the connectors must be able to connect to a domain controller that can be resolved by its DNS name and has port 389 opened for LDAP connections, and has port 445 opened for SMB connections.

   If the domain is verified successfully, click **Close**.

If you have configured subnet mapping for connectors, you might need to modify the subnet settings to ensure you have a connector that can access an appropriate domain controller.

Adding Active Directory Domain Accounts

After you display the details for a selected domain, you can click Accounts to view, add, modify, or delete the Active Directory accounts used to access computers in the selected domain. In order to add domain accounts, you must have the Add Account permission enabled (see the Add Account permission in "Additional domain permissions."

To add a new account for a domain:

1. In the Admin Portal, click ***Resources**> **Domains** to display the list of domains.
2. Select the domain to display the domain details.
3. Click **Accounts**, then click **Add**.
4. Type the user name and password for the account you want to use to access the currently selected domain.

   Note: Note that you should specify the user name by typing the userPrincipalName account attribute.

5. Select the **Manage this credential** or **Manage password using administrative account** (if an administrative account is configured for the domain) option if you want the Privileged Access Service to manage the password for the specified account.

   If you select this option, the Privileged Access Service will automatically update the password after you successfully add the account.

Manage password using administrative account is only displayed if an Administrative Account is configured for the domain and *Enable automatic account maintenance using administrative account* domain policy is enabled. This option is selected by default. If there is no password configured for the account, Privileged Access Service checks to make sure the account is valid and then resets the password. Also, see "Setting Domain-specific Policies" on page 491.

6. Optionally, type a description for the account, then click **Add**.

Managed Passwords and Password Complexity

For any account you add, you can also choose whether or not you want the Privileged Access Service to manage the account password. If you select **Manage this credential**, the Privileged Access Service automatically resets the password after the account and system are added and each time the account is checked in.

All managed passwords generated by the Privileged Access Service consist of at least one upper case letter, one lower case letter, one number, and one special character regardless of the system type. For Windows domain accounts, the following additional password rules apply:

- Minimum password length: 12 characters.
- Maximum password length: 32 characters.
- Supported special characters: !$%&()*+,-./:;<=>?[]^_{|}~
- Only characters that are standard ASCII characters are supported.

You should keep in mind that only the Privileged Access Service will know the managed password being generated and stored. You should not select this option if you don't want the Privileged Access Service to manage the password for the account.

Adding Domain Sets

After you have added domains, you can organize them into logical groups—domain sets—to simplify management activity and reporting for domains with attributes in common.

To add a domain set:

1. In the Admin Portal, click **Resources**, then **Domains** to display the list of domains.
2. In the Sets section, click **Add** to create a new set.
3. Type a name for the new set, an optional description, and select whether group membership is manual or dynamic.

   For manual sets, you can specify permissions for both the set itself and the members of the set. For dynamic sets, you can only specify permissions on the set.
4. Identify the members of the set in one of two ways.
   - If set membership is **Dynamic**, type the SQL statement to execute to identify set members in the **Query** field. For example, if you want to add a set for the domains with a name that starts with pub, you could type a SQL statement like this:

```
select id from vaultDomain where name like 'pub%'
```

- If you select **Manual**, click **Members**, then click **Add** to search for and select the systems to add as members.

5. Click **Save**.

Adding Child Domains

You can add a child domain under a parent domain to form a parent tree in the **Domain** tab.

To add a child domain

1. In the Admin Portal, click **Resources**, then click **Domains** to display the list of domains.
2. Select the domain that you want to add a child domain under.
3. Click the **Actions** menu, then click **Add Child Domain**. The Actions drop-down list becomes available after you select a domain.
4. Type the child domain name and, optionally, a description to identify the domain.
5. Optionally, select **Verify Domain** to test access to the domain, then click **Add**.

   If the domain is verified successfully, click **Close**.

Setting Domain-specific Advanced Options

Setting Options

You can set advanced security and maintenance settings for individual domains or domain sets. You can also set security and maintenance options globally to apply to all domains except where you have explicitly defined a domain-specific setting. If you use a combination of global and domain-specific settings, the domain-specific settings take precedence over the global settings.

If you are not using global security settings or want to override global settings on specific domains, you can set the following advanced security and maintenance options on a case-by-case basis:

- "Set domain administrative accounts"
- "Enable automatic account maintenance using the administrative account"
- "Enable manual account unlock using the administrative account"
- "Allow multiple password checkouts"
- "Enable periodic password rotation"
- "Enable password rotation after checkin"
- "Minimum password age"
- "Password complexity profile"
- "Enable periodic password history cleanup"

In addition, the Privileged Access Service periodically updates the “joined zone” status of systems in the domain. You can view and change the update interval for all systems in the domain using the following Domain/Zone Tasks:

- "Enable periodic domain/zone joined check"
- "Enable periodic removal of expired zone role assignments"

To set domain-specific advanced options:

1. In the Admin Portal, click **Resources**, then click **Domains** to display the list of domains.
2. Select the domain to display the domain-specific details.
3. Click **Advanced**.
4. Select settings for any or all of the advanced domain options.
5. Click **Save**.

For more information about how to set the domain-specific options, click the information icon in the Admin Portal.

Allowing Multiple Password Checkouts

Select No for **Allow multiple password checkouts per AD account added for this domain** if only one administrator is allowed check out the password for a selected domain at any given time. If you select No, the administrator must check the password in and have a new password generated before another administrator can access the domain computers with a domain account and the updated password.

Select Yes if you want to allow multiple users to have the account password checked out at the same time for a selected domain. If you select Yes, multiple administrators can access the domain with a domain account without waiting for the password to be checked in.

Enabling Periodic Password History Cleanup

Select Yes to automatically delete retired passwords from the password history after a given number of days. Select No to prevent the Privileged Access Service from automatically deleting retired passwords from the password history at a set interval.

If you select yes, you can also specify the maximum number of days of password history to keep. For example, if you have a requirement to keep a record of passwords used for three years, you might set the cleanup interval to 1096 days to maintain the password history for that period of time. If you select the default setting, retired passwords are automatically deleted after 365 days. You cannot set a cleanup interval less than 90 days.

Enabling Periodic Password Rotation

Select **Yes** if you want to rotate managed passwords automatically at the interval you specify. Select No if you want to prevent password rotation for the selected system.

If you select **Yes**, you should also specify the password rotation interval in days. Type the maximum number of days to allow between automated password changes for managed accounts. You can set this policy to comply with your organization's password expiration policies. For example, your organization might require passwords to be changed every 90 days. You can use this policy to automatically update managed passwords at a maximum of every 90 days. If the policy is not defined, passwords are not rotated.

Enabling Password Rotation After Check-in

After you check out a managed password for a domain computer, you can specify whether the managed password is rotated after it is checked in.

Select **Yes** to allow password rotation after password check in. Select **No** to not allow password rotation after it is checked in. Select --* to use the default setting from the Security Settings in the Settings tab.

Minimum Password Age

Specify the minimum number of days that a managed password must have been in use before it can be rotated.

Password Complexity Profile

Select an existing password generation profile or add a new profile for the selected domain. If you don't select or add a profile, the default password generation profile for the domain is used. For more information about adding and editing password complexity profiles, see "Configuring password profiles."

Enabling Periodic Domain or Zone Joined Check

Select to periodically update the zone joined status of systems in the domain. If you do not enable this option, the Privileged Access Service does not automatically update the zone joined status of systems in the domain at a set interval.

If you enable to periodically update the domain/zone joined status, you also specify the frequency in minutes for the status refresh. If you do not specify an interval, the default interval is 60 minutes.

Enabling Periodic Removal of Expired Zone Role Assignments

Select to set an interval at which expired zone role assignments are automatically removed from Active Directory. Do not select if you want to prevent expired zone role assignments from being automatically removed from Active Directory.

If you select to enable the removal of expired zone role assignments, you also specify the interval for the removal frequency in days. If you do not specify a value, the default interval is 6 days.

Setting Domain-specific Permissions

You can set permissions for individual domains or on the members of a set of domains. You can also set account permissions for the accounts used to access domains.

To set domain-specific permissions:

1. In the Admin Portal > **Resources** > **Domains** to display the list of domains.
2. Select the domain to display the domain details.
3. Click **Permissions**.
4. Click Add to search for and select the users, groups, or roles, to which you want to grant domain-specific permissions, then click **Add**.
5. Select the appropriate permissions for each user, group, or role you have added, then click **Save**.

For more specific information about what different permissions allow users to do, see "Setting Global Account Permissions" on page 750.

Setting Domain-specific Policies

Setting Policies

You can set the following domain policy for individual domains or domain sets:

"Checkout lifetime (minutes)"

To set domain-specific policies:

1. In the Admin Portal > **Resources** > **Domains** to display the list of domains.
2. Select the domain to display the domain-specific details.
3. Click **Policy**.
4. Select settings for any or all of the domain policies.
5. Click **Save**.

For more information about how to set the domain policies, click the policy link or the information icon in the Admin Portal.

Checkout Lifetime

Type the maximum number of minutes administrators are allowed to have a password checked out. After the number of minutes specified, the Privileged Access Service automatically checks the password back in. The minimum checkout lifetime is 15 minutes. If the policy is not defined, the default checkout lifetime is 60 minutes.

You can extend the checkout time for a password as long as you do so before the initial checkout period expires. For example, if the maximum checkout lifetime is 60 minutes and you extend the checkout time before the 60 minute period is over, the password expiration is reset to the 60 minute checkout lifetime. For more information about configuring the Checkout lifetime policy, see "Extending the password checkout time."

Enabling Manual Account Unlock

On the **Admin Portal > Domains > Advanced** page, you can configure Privileged Access Service to manually unlock account passwords for domain accounts and local accounts on domain-joined Windows systems using the domain administrative account. This requires users to have the Unlock Account permission set at the domain level. Under **Enable Manual Account Unlock** you can enable the following:

- Domain Accounts

  Enables users with the proper permissions to use the domain administrative account to manually unlock managed domain account passwords stored in Privileged Access Service.

- Local Accounts

  Enables users with the proper permissions to use the domain administrative account to manually unlock passwords for managed local accounts on domain-joined Windows systems stored in Privileged Access Service. For information on setting up local system account password reconciliation, see "Configuring Domains for Local Account Password Reconciliation" on page 549. Make sure the corresponding local account

setting is also enabled in Systems> Advanced > Local Account Manual Unlock see "Setting System-specific Advanced Options" on page 561.

Before enabling this policy you need to:

- Set up an administrative account for the domain.

  For information on configuring an administrative account for a domain, see "Setting Domain Admin Accounts" on the next page.

- Configure the domain user to have the Unlock Account permission.

  For information on configuring the Unlock Account permission, see "Setting Global Account Permissions" on page 750.

- Make sure the domain user account is a managed account.

  For information on setting up a domain account with a managed password, see "Adding Active Directory Domain Accounts" on page 486.

Note: If an account that is set as the Privileged Access Service administrative account for the domain is locked, that account cannot be unlocked. An administrative account cannot unlock itself. For instance, if maria.garcia@cpubs.net is locked, the administrative account assigned to cpubs.net is used to unlock the account. However, if maria.garcia@cpubs.net is set to be the administrative account, the account cannot be unlocked.

Enabling Automatic Account Maintenance

On the Domains > Advanced page, you can configure Privileged Access Service to perform automatic account maintenance for domain and local accounts. Under **Enable Automatic Account Maintenance** you can enable the following:

- Domain Accounts

  Enables Privileged Access Service to manage passwords for managed domain user accounts. Privileged Access Service detects an out-of-sync password for a managed domain user account during password rotation, login, and checkout. Also, when this policy is enabled and the administrative account is configured, a managed domain user account can be added without a password configured; Privileged Access Service automatically resets the password associated with the domain user account.

- Local Accounts

  Enables Privileged Access Service to manage passwords for local system accounts on domain-joined Windows systems. Using the domain administrative account, users with the proper permissions can reset out-of-sync account passwords stored in Privileged Access Service. Privileged Access Service detects an out-of-sync password for a managed local system account during password rotation, login, and checkout. Also, when this policy is enabled and the administrative account is configured, a managed local system account can be added without a password configured; Privileged Access Service automatically resets the password associated with the local system account. For information on setting up local system account password reconciliation, see "Configuring Windows local account reconciliation."

  Make sure to enable the corresponding policy in **Resources > Systems > Advanced** see "Setting System-specific Advanced Options" on page 561.

Before enabling this policy you need to:

- Set up an administrative account for the domain.

  For information on configuring an administrative account for a domain, see "Setting Domain Admin Accounts" below.

- Make sure the domain user account is a managed account.

  For information on setting up a domain account with a managed password, see "Adding Active Directory Domain Accounts" on page 486.

Resetting out-of-sync passwords and unlocking managed accounts does not change the domain account privileges or access to data.

[title]: (Domain Admin Acts) [tags]: # (pas,domain,admin accounts) [priority]: # (1000)

Setting Domain Admin Accounts

You can store Active Directory domain administrative accounts in the Privileged Access Service to:

- Enable zone role workflow

  You can use the domain administrative account to configure a workflow that allows users to request role access to systems. For more information, see Managing zone role assignment requests.

- Unlock a locked managed domain account or local accounts on domain-joined Windows systems

  You can use the domain administrative account to configure Privileged Access Service to manually unlock managed domain accounts and local accounts on domain-joined Windows systems (see "Enable manual account unlock using the administrative account." The appropriate policies for the domain and the Windows system must also be configured to unlock accounts.

- Manage domain accounts or local accounts on domain-joined Windows systems

  You can use the domain administrative account to ensure that Privileged Access Service can always successfully manage the passwords for domain accounts and local accounts on domain-joined Windows systems, regardless of whether the account password is out of sync. Note that the Administrative account cannot change it's own password if the minimum password age is not met. For more information, see "Enable automatic account maintenance using the administrative account."

You can also set multiple administrative accounts within the same domain, to address different sets of accounts.

The stored accounts can be any user or service account that has domain or enterprise administrator permissions.

The following requirements must be met before you can store domain administrative accounts on Privileged Access Service:

- Your tenant must have a live connector configured.
- You must know the password of the account you are storing as a domain administrative account.
- Edit and Add Account permissions must be configured for the selected domain.
- Account has the proper delegation controls configured or is part of the Domain Admins group. See "To configure delegation control in the domain controller for the administrative account ."
- If the domain administrative account is used to manage local accounts on domain-joined Windows systems, it must be a member of the Administrators group on the system. By default, the AD Domain Admins group is a member of the local Administrators group.

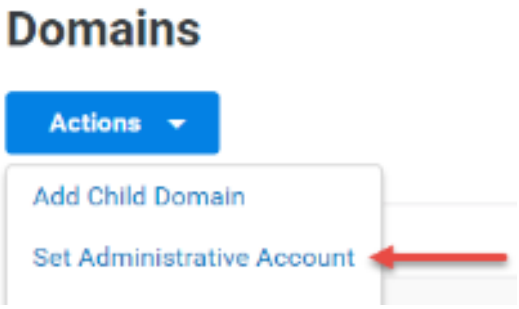
The Privileged Access Service cannot reconcile domain administrative account passwords that may be locked or out of sync. If the domain administrative account encounters an issue, operations using the domain administrative account will fail and an error message is displayed when you browse to the ***Resources*** portion of the Admin Portal. To troubleshoot the issue, see "Troubleshooting domain administrative accounts."

To set domain administrative accounts:

1. In the Admin Portal, click **Resources**, then click **Domains** to display the list of domains.

   Discovered domains, synced domains (with an active connector) and manually added domains are displayed.
2. Select the domain or multiple domains that contain the account you want stored from the domain list.

   Selecting one or more domains activates the Actions menu.
3. Click the **Actions** menu, then click **Set Administrative Account**.



   The selected domain and the administrative account can be from different domains within the same forest.
4. Select the source of the account (**Privilege Service** or **Active Directory**).

   If you are setting up an administrative account for a manually added domain or a domain that was discovered, you can only choose from Privilege Service Accounts. The *Discovered* column in the Domains tab displays the following values:

Discovered Column Value	Add Domain Method	Administrative Account Source
Auto	Domain automatically synced	Privilege Service or Active Directory
Time stamp	Domain discovery	Privilege Service
Blank	Domain manually added	Privilege Service

5. Click **Select** next to the Account text box to select the relevant account.
6. Start typing the account name into the search box.

   Domain accounts that you have Grant rights to are displayed.
7. Select the account you want to store.
8. Click **Add** and then click **Save**.

   The relevant account is displayed in the Administrative Account column.

Note: You can alternatively set up an administrative account for a domain in the Domains > Advanced page. Click **Resources** > **Domains** > **Advanced** and then click **Select** next to the Administrative Account text box.

To clear domain administrative accounts:

1. In the Admin Portal, click **Resources**, then click **Domains** to display the list of domains.
2. Select the domain that contains the account you want to remove as an administrative account for the domain.
3. Click the **Actions** menu, then click **Clear Administrative Account**. The Actions drop-down list becomes available after you select a domain.

Note: You can alternatively clear an administrative account for a domain in the Domain Advanced page. Click **Resources** > **Domains** > **Domain Name** > Advanced and then click **Clear** next to the Administrative Account text box. You can also select **Clear Administrative Account** from the Actions menu on the Domain Advanced page.

To set multiple administrative accounts within the same domain:

1. In the Admin Portal, click **Access** > **Policies** > **Add Policy Set**.
2. On the Policy Settings page:
   a. Under **Policy Assignment**, select the**Sets** option.
   b. Ensure the **Set Type** is set to **Account**.
   c. Under the **Sets** dropdown, select **Domain Accounts**.
3. On the Resources > Accounts page, scroll down to **Account Reconciliation Settings** > **Domain Administrative Account**.
4. Click the **Set** button and use the **Select** button open the search window
5. Use the search field to find the administrative account you want to add and click **Select**.
6. Click **Select** to set the Domain Administrative Account.

Note: You can use Policy Settings to set a specific domain administrative account to specific domain account.

Configuring Admin Account Delegation Control

If you use a regular domain account (not part of the Domain Admins group) for the administrative account, you need to configure the domain account with the proper rights delegation in the domain controller.

Note: The delegated permissions configured for the administrative account are not available for some protected groups. See the following for details: https://support.microsoft.com/en-us/help/817433/delegated-permissions-are-not-available-and-inheritance-is-automatical

To enable delegated permissions on the administrative account to manage protected groups, see the additional configuration steps in "To configure delegation control in the domain controller for protected group accounts ."

To configure delegation control in the domain controller for the administrative account

1. In the domain controller of the domain, select **Administrative Tools > Active Directory Users and Computers**.
2. Right-click the domain with the accounts to be managed and select **Delegate Control**, and then click **Next** at the Welcome window.
3. At Users and Groups, click **Add** and enter the name of the user you want to configure with the administrative account (with unlock and password reset permissions) and click **OK**.
4. In Task to Delegate, select **Create a custom task to delegate** and click **Next**.
5. In Active Directory Object Type, select **Only the following objects in the folder**, and select **User objects** and then click **Next**.
6. In Permissions, select the following:
   - **General** and **Reset password** to delegate password reset rights.
   - **Property-specific**, **Read msDS-User-Account-Control-Computed**, **Read lockout Time**, **Write lockout Time** to delegate account unlock rights.
7. Click **Next** and then **Finish**.

   The domain account with delegated permissions can now be configured as the domain administrative account for the account unlock and automatic account maintenance features.

To configure delegation control in the domain controller for protected group accounts

1. At a command prompt on the domain controller, type the following command to grant the domain account permission to perform account unlock.

   Note: dc=cps and dc=com in the following commands should be changed to your domain name.

   ```
   dsacls "dc=cps,dc=com" /G "<yourDomainName>\<yourAccountName>:RP;msDS-User-Account-
   Control-Computed;user" /I:S
   ```

   ```
   dsacls "dc=cps,dc=com" /G "<yourDomainName>\yourAccountName>:RPWP;lockoutTime;user" /I:S
   ```

   ```
   dsacls "CN=AdminSDHolder, CN=System, DC=cps, DC=com"  /G
   "<yourDomainName>\<yourAccountName>:RPWP;lockoutTime"
   ```

2. At a command prompt on the domain controller, type the following command to grant the domain account permission to perform password reset.

   Note: dc=cps and dc=com in the following commands should be changed to your domain name.

   ```
   dsacls "dc=cps,dc=com" /G "<yourDomainName>\<yourACcountName>:CA;Reset Password;user"
   /I:S
   ```

```
dsacls "CN=AdminSDHolder, CN=System, DC=cps, DC=com"  /G
"<yourDomainName>\<yourAccountName>:CA;Reset Password"
```

It can take a while for the Security Descriptor Propagator Update (SDProp) process to pick up the new settings from AdminSDFolder. To initiate the SDProp process immediately, complete the following steps:

1. Click **Run** and enter ldp.exe in the domain controller desktop Start menu.
2. Select **Connection > Connect...** from the Ldp window.
3. In the Connect window, make sure **389** is listed in the Port field, and then click **OK**.
4. Select **Connection > Bind...** from the Ldp window.
5. Select **Bind as currently logged on user** and click **OK**.
6. Select **Browse > Modify** from the Ldp window.
7. Configure the following fields in the Modify window:

   DN field: empty

   Attribute field: type RunProtectAdminGroupsTask

   Values field: 1

   Operation: click **Add** and then click **Enter**.
8. Click **Run**.

   If you have a large environment, it may take some time for SDProp to update the protected admin group permissions.

Troubleshooting Domain Admin Accounts

The Privileged Access Service cannot reconcile domain administrative account passwords that may be locked or out of sync. If the domain administrative account encounters an issue, operations using the domain administrative account will fail and an error message is displayed when you browse to the **Resources** portion of the Admin Portal. To troubleshoot the issue, see the following:

Issue	Description	Troubleshoot
Insufficient Permissions	The administrative account has insufficient access rights to perform the required operation on a domain account.For example, if the administrative account does not have permission to reset domain account passwords, the managed domain account password cannot be rotated.	If you suspect that the administrative account has insufficient permissions, check for proper account permissions in your domain controller. Navigate to **Properties > Member of...** to check administrative account's group configuration. Then, navigate to **Properties > Security** (you may need to enable View > Advanced Features) for the managed account, and check the permissions for that group. Once you correct the issue, you can click the X in the banner to dismiss it.
Invalid credentials	The administrative account may have invalid credentials due to: Multiple logins with invalid credentials causing the account to lock. Disabled or deleted account. Non-existent domain account. Expired or out-of-sync password. Password update required at the next logon.	If you suspect the account has invalid credentials, you can run a check on the domain administrative account in Privileged Access Service to verify the password, or check the credentials of that account in the domain controller directly. In the domain controller you can: Enable the account if it was disabled. Reset the account password and unlock the account (if it was locked) in domain controller. Then, update the account password in Privileged Access Service. Change the administrative account to use an account that does exist in the domain (if the account did not exist in the domain).Once you correct the issue, you can click the X in the banner to dismiss it.

Planning Domains and Domain Accounts

Before adding domains to the Privileged Access Service, you might want to consider which Active Directory accounts you want to manage and whether there are specific privileges you should be aware of when deciding which account passwords you want stored and managed using the Privileged Access Service.

The most likely candidates for being managed accounts are Active Directory administrative accounts and application service accounts. You can use the Privileged Access Service to manage the password for any of these accounts or add any other accounts of your choice to securely store the account information without having the password managed by the Privileged Access Service.

You should note, however, that you must add domain accounts to the domain where they belong. For example, if you want to manage a domain account that is in a child domain instead of the forest root domain, you must add the child domain to the Privileged Access Service first, then add the domain accounts you want to manage for the child domain under the child domain.

Selecting Connectors

By default, domains use any available connector without evaluating the network topology. If the communication with a current connector is interrupted, the domain automatically selects another available connector to continue operation. To give you more control over which connector different computers use, you can map specific subnet patterns to specific connectors. Domain computers can then use the globally-defined network topology to identify the closest connector available and will use the next closest available connector if the communication with the closest connector is interrupted.

Using Subnet Grouping with Domains

If you organize systems by grouping them into domains, you can optimize the connector selection by using the domain as another layer of filtering to choose a connector. Using domains within subnet groups is more efficient than using the subnet grouping without any additional filtering.

When a connector is required to perform an operation for any system, the connector selected is determined by doing the following:

- If the computer is configured to use a connector based on the subnet group and the system address is defined using the system IP address, the IP address to subnet mapping is used to select the connector.
- If system address is defined using a fully-qualified domain name (FQDN) and not the IP address, the domain setting is used to select the appropriate connector for the domain.
- If the domain is not explicitly set for the system but the domain exists in the Privileged Access Service, the domain portion of the system address is used to select the appropriate connector.

Using the domain setting with subnet mapping gives you the best combination of performance and failover support in most cases. However, there are circumstances in which you might prefer to specifically designate the connectors individual domains should use. For example, if the “closest” connector in the network topology has bandwidth or latency issues, you might want to designate only one or more specific connectors for an individual domain.

If you want to specify the connectors for an individual domain, you can do so when viewing the details for the domain. Domain-specific settings take precedence over any global connector subnet mapping you have configured. Additionally, if you set system-specific connector settings, those would take precedence over any other domain-specific or subnet mappings that you may have configured.

To specify the connectors to use for a domain:

1. In the Admin Portal > **Resources** > **Domains** to display the list of domains.
2. Select the domain to display the domain details.
3. Click **Connectors**.
4. Select **Choose**, then select the specific connectors to use for the domain from the list of available connectors.
5. Click **Save**.

Adding Secrets

Secrets are stored as one of the following types:

- Text: The raw text option is useful for storing private keys for secure shell sessions, connecting to file transfer servers, managing a common API key for a subscription service, or accessing cloud-based storage. Because the text string is encrypted for storage, the maximum size of the raw text is 24KB. For text strings that exceed this limit, you should upload them as secret files.
- File: The file option is useful if you have spreadsheets, image files, or other types of documents that contain sensitive or confidential information, include multiple private access or application license keys, or record administrative account information.

After you upload a secrets, you can set permissions on them directly or organize them into sets or folders to simplify other tasks such as assigning set or folder-specific permissions.

Adding New Secrets

You can add a secret one of two ways: either by dragging and dropping the secret file onto the secrets page or uploading it by way of adding it.

Adding Secret by Drag and Drop

To drag and drop a secret, navigate to **Resources** > **Secrets** and you can drag and drop the secret.

Adding Secrets

1. In the Admin Portal, click **Resources**, then click **Secrets** to display the list of secrets.
2. Click **Add Secret**.
3. Type the display name and, optionally, a description to identify the secret.

   You can type a path to create folders and subfolders to organize your secrets. For example, in the Name field type *Production/DevSys/mysecret*. This creates a secret (text or file) with the filename *mysecret* in the folder *Production/DevSys*.

   You can also create subfolders and secrets in a folder that already exists. For instance, if the folder *Production* already exists, typing *Production/DevSys/mysecret* in the Name field creates the subfolder *DevSys* and the secret *mysecret* under the folder *Production*. In this case, you need to have the **Add** permission for the *Production* folder.
4. Select **Text** or **File** from the Type drop-down menu.
   - For Text, click **Enter Text** and type or paste the text string in the **Secret** field. The text string limit is 24KB.
   - For File, click **Select File** and then browse to and select the file you want to upload. You can select any type of file to upload up to a maximum size of 5MB.
5. At **Add To Set**, you can optionally add the secret an already configured set from the drop-down menu. For more information on sets, see "Adding Secret Sets" on page 502
6. Click **Save**.

   For additional configuration information, see:

   - "Setting Secret, Folder, and Set Permissions" on page 503

Setting Access Challenge Policies

You can set access challenge policies for individual secrets or folders. For example, you might want to require multi-factor authentication for users who have permission to view, edit, retrieve, or replace secrets if certain conditions are met.

An authentication rule specifies the conditions to be evaluated and the authentication profile specifies the challenges presented when the conditions specified are true. You can configure new authentication rules and authentication profiles just for secrets and folders or select and use rules and profiles you have previously created.

Policy Inheritance

Also note the following behavior for multi-factor authentication inheritance:

- Multi-factor authentication policies are inherited and apply to Retrieve, Move, and Delete actions for folders and secrets.
- Folders and secrets take on authentication policies of the closest parent. For instance, a secret in Production/DevSys will take on the policies of the folder DevSys, not Production, if no polices are applied to the secret.
- Multi-factor authentication policies set for a folder or secret, take precedence over any policy set for a parent folder.

To set access policies for secrets and folders:

1. In the Admin Portal, click **Resources**, then click **Secrets** to display the list of secrets or folders.
2. Select the secret or folder to display its details.
   - For Secrets, click the secret to display its details.
   - For Folders, click the check box next to the folder name and then click **Edit** from the Actions menu.
3. Click **Policy**.
4. Select a default access challenge profile, if an appropriate profile exists, or click **Add Rule** to configure one or more authentication challenge rules.
5. Click **Save**.

For more information about how to configure authentication rules and profiles, see "Creating Authentication Rules" on page 281 and "Creating Authentication Profiles" on page 284

Adding Secret Folders

In addition to creating and storing secrets, you can create folders to categorize and manage text and file secrets. Folders can be one folder at the top level or multiple folders nested in a hierarchy. Similar to Sets, folders allow you to create secrets within folders as a way to logically group various secrets. Secrets that are not contained within a folder are shown on the top level of the Admin Portal Secrets page (see "Managing Secrets" on page 677.) If you do not have the proper permissions on a folder that contains a shared secret, the secret is also displayed on the top level of the Admin Portal Secrets page.

Any user with Privileged Access Service rights/roles can create a folder or a secret. If you are the owner of a folder because you created it, you have all permissions (Add, Grant, View, Edit, and Delete) enabled for that folder. In order to create a secret in a particular folder you need to have the **Add** permission for that folder. Users with the System Administrator role have Grant, View, Edit, Delete permissions by default for all secrets within folders.

Also keep in mind the following:

- A secret can belong to only one folder.
- You cannot create two folders with the same name and path.
- You cannot add folders to Secret Sets.
- Folder names are *not* case sensitive (in other words you cannot create two folders with the name Production and production).

You can also add folders when you add a secret, see "Adding Secrets" on page 499 for details.

To add a new folder:

1. In the Admin Portal, click **Resource**, then click **Secrets**.
2. Click **Add Folder**.
3. Type the name of the folder and, optionally, a description to provide additional information about the folder.

   You can also type in a hierarchical path to create multiple nested folders all at once. For instance, in the name field you can enter, Production/DevSys/Temp to create two nested folders under Production. Each folder can contain any number of secrets of type text or file.

   Note: If the folder name you type into the Name field already exists (even if the folder is not viewable), an error is displayed and the folder is not created.

4. Click **Save**.

   For additional information on folders, see:

   - "Setting Secret, Folder, and Set Permissions" on the next page
   - "Setting Access Challenge Policies" on the previous page
   - "Viewing and Changing Settings" on page 680
   - "Moving Secrets and Folders" on page 678
   - "Deleting Secrets or Folders" on page 678
   - "Viewing System Activity" on page 691

Adding Secret Sets

After you have added text strings or files as secrets, you can organize them into logical groups—sets—to simplify management activity and reporting for secrets with attributes in common. You can include both text and files in the same set.

Note: You cannot add folders to Secret Sets.

To add a secret set:

1. In the Admin Portal, click **Resources**, then click **Secrets**, then click **Sets**.
2. Click **Add** to create a new set.
3. Type a name for the new set, an optional description, and select whether group membership is manual or dynamic.

   For manual sets, you can specify permissions for both the set itself and the members of the set. For dynamic sets, you can only specify permissions on the set.
4. Identify the members of the set.
   - If you select **Manual**, click **Members**, then click **Add** to search for and select the secrets to add as members.
   - If set membership is **Dynamic**, type the SQL statement to execute to identify set members in the **Query** field. For example, if you want to add a set for the secrets with a name that starts with api, you could type a SQL statement like this:

     ```
     select id from DataVault where SecretName like 'api%'
     ```
5. Click **Save**.

For information about changing sets after you have added them, see "Modifying Sets" on page 685

Enabling Secret Workflow

To provide “retrieve secrets” workflow for secrets, you can enable secrets workflow as a feature that applies to secrets stored in the Privileged Access Service. You can also use the global setting in conjunction with the following secret-specific settings to restrict access requests for some secrets or modify the user or role with approval authority.

To enable secrets workflow for a specific secret

1. In the Admin Portal, click **Resources** > **Secrets** to list all the secrets.
2. From the list of secrets or secrets in any folders, select the specific secret for which you want to enable workflow.
3. In the **Enable Secret Workflow** dropdown, select **Yes**.
4. From the **Approver List**, select either **Requestor'sManager** or **Specified User or Role**.

   Note: If using Requestor's Manager approver, and the requestor has no manager, you can select automatically approve, deny, or route to another user/role.
5. Click **Add** and select user and role.
6. Once added, click **Save**.

Setting Secret, Folder, and Set Permissions

You can set permissions for the following secret objects:

- Individual secrets (text or file)

  Secret permissions control access to the secret (text or file) and what actions are available to the user. If you created the secret, by default you have all permissions to the secret.

- Folders

  Folder permissions control access to the folder and what folder actions are available to the user. If a user does not have the View permission for the folder, the user will not see the folder in the Admin Portal. Any changes to the folder permissions are also distributed to subfolders in the hierarchy. If you created the folder, by default you have all permissions associated with the folder.

- Folder members

  Member permissions control access to all the secrets in a folder and what actions are available to the user for all secrets in the folder. When new secrets are added to a subfolder, member permissions are distributed to subfolders in the hierarchy.

- Secret Sets

  Secret Set permissions control access to the set of secrets and the actions available to the user. If a user does not have the View permission for the set, the user will not see the set in the Admin Portal. If you created the set, by default you have all permissions associated with the set. For manual sets, you can specify permissions for both the set itself and the members of the set. For dynamic sets, you can only specify permissions on the set.

- Secret Set members

  Member permissions control access to all the secrets in a set and what actions are available to the user for all secrets in the set.

You can also set account permissions for the accounts used to access secrets.

For detailed information on permissions, see "Assigning Permissions" on page 743

To set permissions:

1. In the Admin Portal, click **Resources**, then click **Secrets** to display the list of secrets and folders.
2. Select a secret, folder, or set.
   - For Secrets, click the secret to display its details.
   - For Folders, click the check box next to the folder name and then click **Edit** from the Actions menu.
   - For Sets, right-click the set and then click **Modify**.
3. Click one of the following permission options:
   - Permissions (for secrets and sets)
   - Folder Permissions (for folders)
   - Member Permissions (for folders and sets)
4. Click **Add** to search for and select the users, groups, or roles, to which you want to grant permissions, then click **Add**.

   By default, the user, group, or role is granted the View permission.
5. Select the appropriate additional permissions for each user, group, or role you have added, then click **Save**.

Note that users who inherit their permissions from their membership in the System Administrator role can see the complete list of secrets but cannot retrieve any secrets unless they are explicitly granted the Retrieve Secret permission. In addition to granting explicit permission for Retrieve Secret, and inheriting it from roles and sets, users can also inherit the Retrieve Secret permission from parent folder(s). For more specific information about what different permissions allow users to do, see "Assigning Permissions" on page 743

Note: If you have performed a multi-account delete, the secret file is saved with view only permission until the system administrator has given you rights to perform additional tasks.

Adding Services Manually

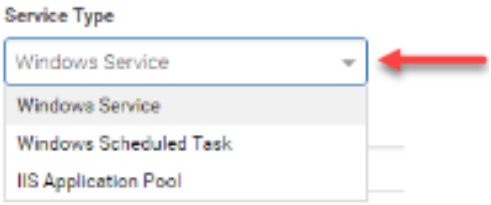
In most cases, you add services to Privileged Access Service by running discovery jobs that scan your network for information about computers in Active Directory domains. However, you can also manually add services on a system-specific basis. To add services manually, you must have the following administrative permissions:

- Edit permission on the target system.
- Checkout permission for the administrative account.
- Checkout and Edit permission for the sub-accounts associated with the multiplexed account for the service.

For more information about setting permissions, see "Setting global system permissions" and "Setting global account permissions." If you want to enable automatic password management for the service, you must also create two new accounts to use as the multiplexed account. For more information about preparing a multiplexed account, see "Adding multiplexed accounts."

To manually add a service:

1. In the Admin Portal, click **Resources** then click **Services** to display the list of services and scheduled tasks.
2. Click Add Service. Alternatively, you can select a system to displays its details, then click **Services** to add a system-specific service.
3. Click **Select** to browse for or change the target system where the service runs.
4. Type an optional description for the service.
5. Select Windows Service, Windows Scheduled Task, or IIS Application Pool as the service type.



6. Type the service name, application pool name, or the full path to the scheduled task. For example, the service name for the Virtual Disk service is vds.
7. Select **Enable management of this application password** if you want the password for the service account to be managed by the Privileged Access Service.

8. This setting requires you to specify an Administrative account in Step 8 and a multiplexed account in Step 9. If you have not yet prepared a multiplexed account, see "Adding Multiplexed Accounts" on page 508 before selecting **Enable management of this application password** for a new service.
9. Click **Select** to search for and select a stored domain account you want to use to manage the password for the service.

   Type a search string to locate an appropriate domain account that is stored in the Privileged Access Service and has the sufficient permissions to modify the service account password.

   Select the account in the list of results, then click **Add**.

   The administrative account is the account that rotates the service account password if you enable automatic password management.
10. Click **Select** to search for and select a multiplexed account to run the service.

    The multiplexed account must meet the following criteria:

    - Its sub-accounts must be domain accounts with passwords stored and managed by the Privileged Access Service.
    - Its sub-accounts must have sufficient permissions to run the Windows service or scheduled task.
    - The domain where the sub-accounts are used must have periodic password rotation enabled and a duration set at the domain or global security settings level.

    You should not use Active Directory Managed Service Accounts or Group Managed Service Accounts as multiplexed accounts.

    You can configure multiplexed accounts for services after running discovery jobs or before or after adding a service manually. You must create multiplexed accounts before you can enable automatic password rotation.
11. Click **Save** to save the service settings.

If changing the account password for a service requires restarting the service, you can have automatically restarted without any time constraints or only on certain days of the week and certain hours of the day. For more information about enforcing time restrictions, see "Setting restart time constraints."

Adding Service Sets

After you have added services, you can organize them into logical groups– service sets–to simplify management activity and reporting for services with attributes in common.

To add a service set:

1. In the Admin Portal, click **Resources**, then **Services** to display the list of Windows services and scheduled tasks.
2. In the Sets section, click **Add** to create a new set.
3. Type a name for the new set, an optional description, and select whether group membership is manual or dynamic.

   For manual sets, you can specify permissions for both the set itself and the members of the set. For dynamic sets, you can only specify permissions on the set.
4. Identify the members of the set in one of two ways.

- If set membership is Dynamic, type the SQL statement to execute to identify set members in the Query field. For example, if you want to add a set for the Windows service with a type that starts with win, you could type a SQL statement like this:

  select id from subscriptions where type like 'win%'

- If you select **Manual**, click **Members**, then click **Add** to search for and select the services to add as members.

5. Click **Save**.

Automating Password Rotation

In most cases, you only configure the multiplexed account for a service if you want to enable automatic password rotation. Automating password rotation for the account used to run a target service requires the service to have both an administrative account and a multiplexed account defined. The **administrative account** is the account that rotates the service account password. The **multiplexed account** is the name used for the two sub-accounts that run an application service or scheduled task.

Because creating the multiplexed account involves adding and testing its sub-accounts, it is typically done some time after you have run a discovery job or have added a service manually.

Before updating a service to enable automated password rotation, you should have completed the following tasks:

- Discovered or added the target service that runs using a specific service account.
- Created and tested the two sub-accounts that will replace the original service account.
- Added the two sub-accounts to the Privileged Access Service with **Manage this credential** selected.
- Enabled the periodic password rotation policy and set an appropriate interval for the domain with the two sub-accounts or as a global security setting.
- Configured the multiplexed account with the two sub-accounts.

If you have completed these tasks, you are ready to update the service to use a multiplexed account.

To automate password rotation for a service:

1. In the Admin Portal, click **Resources > Services** to display the list of services and scheduled tasks.
2. Select a service to view its details.
3. Click **Select** to search for and select the stored domain account that will manage the password for the service, if needed.
4. Type an optional description for the service, if needed.
5. Select **Enable management of this application password**.
6. Select either Windows Service or Windows Scheduled Task as the service type, if needed.
7. Type the application service name or the full path to the scheduled task. For example, the service name for the Virtual Disk service is vds.
8. Click **Select** to search for and select a multiplexed account to run the service.
9. Select **Restart service when password is rotated** if changing the account password requires restarting the service.

10. If you select the Restart option, you can also specify time constraints to control when the service is restarted. For example, you might want to only allow a service to be restarted on Sundays between 2:00AM and 3:00AM based on the local time zone.
11. Click **Save** to save the service settings.

Adding Multiplexed Accounts

Multiplexed accounts are required to enable automated password rotation for the service accounts that run Windows services or scheduled tasks. The multiplexed account has two **sub-accounts** that ensure the account password is synchronized to the same password on all of the computers where it is used before the password is rotated. The multiplexed account prevents a service account that runs on multiple target systems from having its password changed on some systems and not on others and causing service failures.

The sub-accounts for the multiplexed account must meet the following criteria:

- Each account must be a domain account with its password stored and managed by the Privileged Access Service.
- Each account must have sufficient permissions to run the target Windows service or scheduled task.
- Each account must have Checkout and Edit permission.
- Each account must have the “Log on as a service” user right assigned in a local or domain policy if used to run an application service or the “Log on as a batch job” user right if used to run a scheduled task.
- The domain where the sub-accounts are used must have periodic password rotation enabled and an interval set at the domain or global security settings level.

Configuring Multiplexed Accounts

After you create one or more multiplexed accounts, you might need to update the sub-accounts associated with the account. For example, if you have added a new service that should run under the same multiplexed account as another service, you might need to change the sub-accounts to accounts with different permissions.

To change multiplexed accounts:

1. In the Admin Portal, click **Resources**, then click **Accounts** to display the list of accounts.
2. Click **Multiplexed Accounts**.
3. Select the account to display the account-specific details on the Settings page.
4. Click **Select** for Account 1 to search for and select a stored domain account that is managed by the Privileged Access Service.
   - The domain account you select must have the appropriate permissions to run the target service or scheduled task.
   - The domain account password must be managed by the Privileged Access Service.
   - You must have periodic password rotation enabled at the domain or global security settings level.

   When you type a search string to locate the account, only accounts that meet the criteria and are not already associated with another multiplexed account are returned. Select the appropriate sub-account in the list of results, then click **Add**.

5. Click **Select** for Account 2 to search for and select a stored domain account that is managed by the Privileged Access Service.
6. Click **Save** to save the sub-account changes for the multiplexed account.

Creating Multiplexed Accounts

After you have replicated and tested the sub-accounts for a service, you can create a multiplexed account to run one or more target services on one or more target systems.

To create the multiplexed account

1. In the Admin Portal, click **Resources**, then click **Accounts** to display the list of accounts.
2. Click **Multiplexed Accounts**.
3. Click **Add Multiplexed Account**.
4. Type a name and, optionally, a description for the multiplexed account.
5. Click **Select** for Account 1 to search for and select a stored domain account that is managed by the Privileged Access Service.
   - The domain account you select must have the appropriate permissions to run the target service or scheduled task.
   - The domain account password must be managed by the Privileged Access Service.
   - You must have periodic password rotation enabled at the domain or global security settings level.

   When you type a search string to locate the account, only accounts that meet the criteria are returned. Select the appropriate sub-account in the list of results, then click **Add**.
6. Click **Select** for Account 2 to search for and select a stored domain account that is managed by the Privileged Access Service.
7. Click **Save** to save the sub-account settings for the multiplexed account.

The multiplex account ensures that all of the computers where the managed service account is used are synchronized before the password is rotated. If your password rotation interval is 90 days, for example, the service might run for 45 days using the subaccount1 managed password, then switch to using the identical subaccount2 managed password.

When the password expires, a new password is generated and all of the computers with a service running under the subaccount2 managed password pick up the new subaccount1 managed password. If there are issues on any computer preventing rotation, rotation is skipped until the issue is fixed.

Setting Multiplexed Account Permissions

You can click Permissions to view and set permissions for a multiplexed account. For example, if you have changed the sub-accounts associated with a multiplexed account, you might need to add and set new permissions on the new sub-account.

To view and set multiplexed account permissions:

1. In the Admin Portal, click **Resources**, then click **Accounts** to display the list of accounts.
2. Click **Multiplexed Accounts**.

3. Select the account to display the account-specific details.
4. Click **Permissions**.
5. Click **Add** to add a new sub-account to the multiplexed account, if needed. If adding a new account, type a search string to locate the account. Select the appropriate sub-account in the list of results, then click **Add**.
6. Select the sub-account users, groups, roles, or computers to which you want to grant permissions.
7. Select the appropriate permissions, then click **Save**.

Replicating Existing Accounts

In most cases, the multiplexed account—with its two sub-accounts—is used to replace a discovered service account. The sub-accounts for the multiplexed account should have exactly the same permissions and administrative rights as the original service account you are replacing. For example, if the target service has a current service account that is an Active Directory domain account with local Administrator rights, you should create two new Active Directory domain accounts with local Administrator rights. If the target service has a current service account that is a local account with Backup Operators privileges, you should create two new **domain** accounts with Backup Operators privileges.

Testing Sub-Accounts

After you create the accounts that will replace an existing service account, you should test both of the sub-accounts running the target service before you create the multiplexed account that will use them. Note that it is important for you to test operations thoroughly for both of the sub-accounts before you attempt to automate password rotation for a target service. After a service is configured to use the multiplexed account, the Privileged Access Service will only use the sub-accounts to run the target service. The original service account will no longer be used.

By testing the sub-accounts first, you can ensure they don't cause service interruptions, service failures, or account locking problems.

Pushing Service Changes

A task running in the background periodically checks for new and updated services. After you add or update a service, it can take up to one hour for the new service or changes to the service to be picked up by the background job and displayed. If you want to start automated password management immediately after adding a service, you can select the service to activate the Actions menu, then select **Push Password Management**.

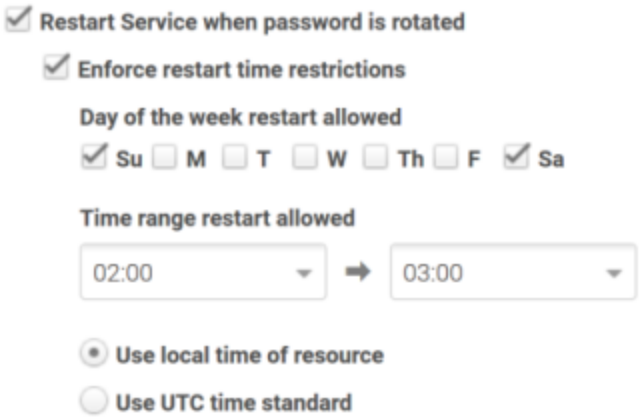
If you have configured time constraints for restarting the application service, you are prompted to confirm that you want to take action immediately.

Setting Restart Time Constraints

You can select **Restart service when password is rotated** if changing the account password for a service requires restarting the service.

If you select the Restart option, you can also select the **Enforce restart time restrictions** option to specify time constraints that will control when the service is restarted. For example, you might want to only allow a service to be restarted on Saturday or Sunday between 2:00AM and 3:00AM based on your local time zone.

For example:



If a service is running under its account when it is time to rotate the password, password rotation is skipped on the system until the service session ends.

If you restrict when a service can be restarted, the same restrictions apply when you attempt to start automated password management on demand by selecting the **Push Password Management** action. For more information about starting password management on demand, see "Pushing Service Changes" on the previous page

Setting Service-specific Permissions

You can set permissions for individual applications or set global permissions to apply to all applications. If you use a combination of global and application-specific permissions, the application-specific permissions take precedence over the global permissions you set.

You can set permissions for individual services or on the members of a set of services. You can also set account permissions for the accounts used to access services.

To set service-specific permissions:

1. In the Admin Portal, click **Resources** > **Services** to display the list of services and scheduled tasks.
2. Select the service to display the service details.
3. Click **Permissions**.
4. Click **Add** to search for and select the users, groups, or roles to which you want to grant service-specific permissions, then click **Add**.
5. Select the appropriate permissions for each user, group, or role you have added, then click **Save**.

   Although you can set the Edit permission for the service, users must also have Edit permission on the target system, Checkout permission for the service administrative account, and Checkout and Edit permission for the sub-accounts associated with the multiplexed account for the service.

For more specific information about what different permissions allow users to do, see "Assigning Permissions" on page 743

Starting Password Management

Because automatic password rotation requires some preparation—to add and test the sub-accounts, to create the multiplexed account for the sub-accounts, and to link the multiplexed account to the appropriate service—you might start password management some time after adding or updating a service.

Although a task running in the background will periodically check for services to manage, you can also attempt to start password management immediately on-demand by selecting the **Push Password Management** action.

To start password management immediately:

1. In the Admin Portal, click **Resources**, then click **Services** to display the list of services and scheduled tasks.
2. Select a service to display the Actions menu.
3. Select **Push Password Management**.
4. Click **Yes** to confirm that you want to update the password immediately. If there are time restrictions for restarting the service that are in effect when you are attempting to start password management, you are prompted to confirm restarting the service.
5. Click **Yes** to continue.
6. Click **Close**.

Adding SSH keys

You can add and store SSH keys in Privileged Access Service. After the keys are added, users with the appropriate permissions can retrieve and use these keys, instead of passwords, to log in to UNIX systems, Generic SSH systems, and network devices.

Privileged Access Service supports PEM and PPK for formatted keys and the following key algorithms:

- DSA
- RSA
- ECDSA
- EdDSA

After adding a key, you can do the following:

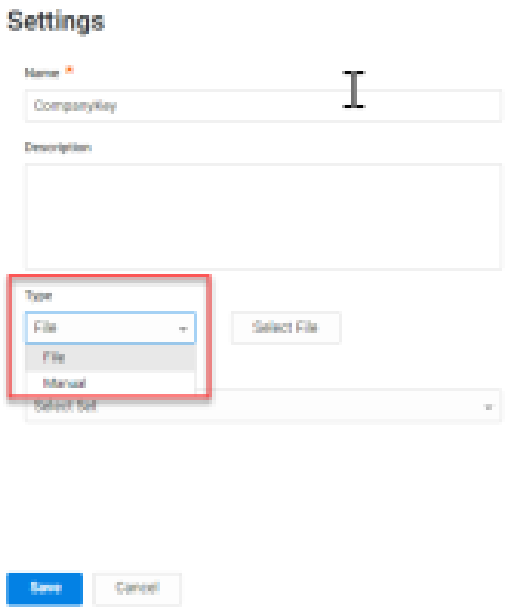
- Assign a SSH key to an account. See "Associating SSH Keys to Accounts" on page 514
- Assign SSH Key management permissions to additional users. See "Assigning SSH Key Management Permissions" on page 517
- Specify additional authentication requirements for retrieving a key. See "Applying Authentication Policies to SSH keys" on page 515
- Retrieve keys for system access. See "Retrieving SSH Keys" on page 473
- See the accounts associated with a key from the Account Usage page. From this page, you can apply specific actions to the account. See "Selecting System Actions" on page 470 for the actions information. Not all actions listed on this documentation page are relevant to a SSH key account type.

There are three ways to add SSH keys:

- Adding the SSH key at the SSH Keys tab (Admin Portal> **Resources** > **SSH Keys** > **Add Key**).
- Dragging and dropping the SSH key at the SSH Key tab (Admin Portal> **Resources** > **SSH Keys** > then drag and drop).
- Upload the SSH key while adding the account (Admin Portal> **Resources** > **Systems** > **Add System**).

Adding an SSH key at the SSH Keys tab:

1. Click **Resources** > **SSH Keys**.
2. Click the **Add Key** button.
3. Enter a **Name** for the key.
4. This name can be updated on the Settings page after you save this key.
5. (Optional) Enter a Description for the key.
6. Select the file type using the Type drop-down list.



7. Selecting **File** allows you to upload a file containing the SSH key:
8. a. Click the **Select File** button.
   b. Navigate to the file location.
   c. Double-click the relevant file.
   d. (Optional) Enter the **Passphrase** associated with the SSH key if you have one.
   e. Click **OK**.
9. Selecting **Manual** allows you to paste a SSH key manually:
10. a. Click the **Enter Key** button.
    b. Paste the SSH private key into the text box.

c. (Optional) Enter the **Passphrase** associated with the SSH key if you have one.

d. Click **OK**.

11. (Optional) Use the **Add to Set** drop-down list to add this key to a set.
12. Click **Save**.

Dragging and dropping an SSH key at the SSH Keys tab:

Navigate to the Admin Portal> **Resources** > **SSH Keys**. At the bottom of the screen there is a drag and drop window that allows you to drag and drop an SSH key.

Uploading the SSH key while adding an account:

For steps on how to upload an SSH key while adding an account, see "Adding Systems with the Wizard" on page 519

Adding SSH Key Sets

After you have added systems, you can organize them into logical groups—SSH key sets—to simplify management activity and reporting for SSH keys with attributes in common.

To add SSH key sets

1. In the Admin Portal, click **Resources**, then click **SSH Keys** to display the list of accounts.
2. In the Sets section, click **Add** to create a new set.
3. Type a name for the new set, an optional description, and select whether group membership is manual or dynamic.

   For manual sets, you can specify permissions for both the set itself and the members of the set. For dynamic sets, you can only specify permissions on the set.
4. Identify the members of the set in one of two ways.
   - If set membership is Dynamic, type the SQL statement to execute to identify set members in the

     Query field. For example, if you want to add a set for the accounts with an account name of root, you could type a SQL statement like this:

     ```
     select id from VaultAccount where name like 'root'
     ```
   - If you select **Manual**, click **Members**, then click **Add** to search for and select the databases to add as members.
5. Click **Save**.

Associating SSH Keys to Accounts

Before users can use a SSH key to log in to a system, you must associate that key to an account. SSH keys can only be associated with accounts for Unix systems, Generic SSH systems, or network devices. Although it is an uncommon use case, you can associate multiple accounts to one key. You use the System tab to associate keys to an account. See "Adding System Accounts" on page 534 for instructions on associating a SSH key to an account.

After you associate a key to an account, that account is populated on the Account Usage page (**Infrastructure** > **SSH Keys** > select a specific key > **Usage**) and on the Accounts page. See "Selecting System Actions" on page 470 for the actions that you can perform on the account.

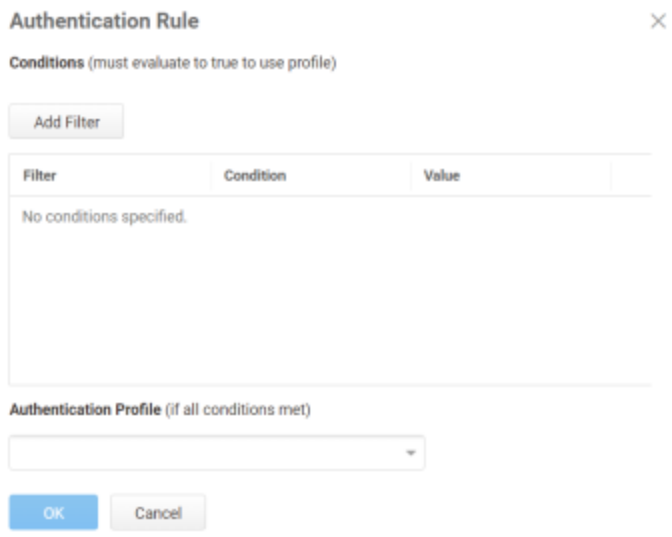
Applying Authentication Policies to SSH keys

You can enforce an authentication rule and profile for retrieving a SSH key. For example, if you apply an authentication rule specify that users attempting to retrieve the SSH key on Saturday or Sunday, then they must meet additional authentication challenges.

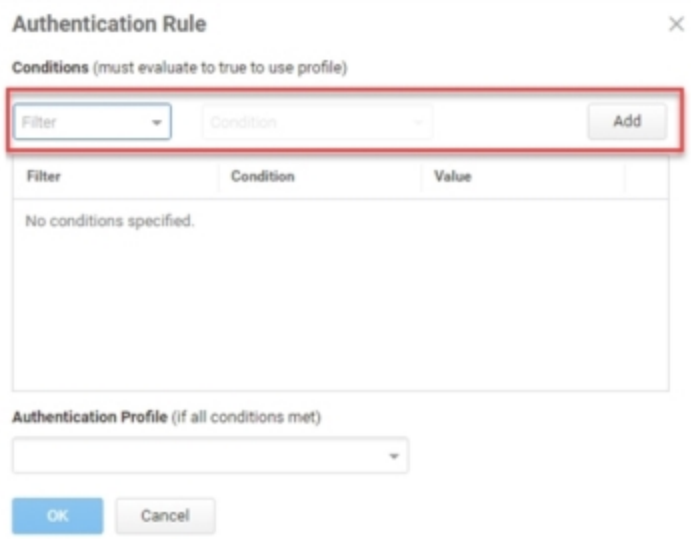
To specify an authentication policy:

1. Click **Resources** > **SSH Keys**.
2. Select the relevant SSH key.
3. Click **Policy**.
4. (Optional) Click **Add Rule** to specify conditional access.

   The Authentication Rule window displays.



5. Click **Add Filter** on the Authentication Rule window.
6. Define the filter and condition using the drop-down menus.



For example, you can create a rule that requires a specific authentication method when users access Privileged Access Service from an IP address that is outside of your corporate IP range. Available filters vary depending on the object they are applied to and features enabled on your tenant. Supported filters are:

Filter	Description
IP Address	The authentication factor is the computer's IP address when the user logs in. This option requires that you have configured the IP address range in Settings, Network, Corporate IP Range.
Identity Cookie	The authentication factor is the cookie that is embedded in the current browser by Privileged Access Service after the user has successfully logged in.
Day of Week	The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.
Date	The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.
Date Range	The authentication factor is a specific date range.
Time Range	The authentication factor is a specific time range in hours and minutes.
Device OS	The authentication factor is the device operating system.

Filter	Description
Browser	The authentication factor is the browser used for opening the Privileged Access Service portal.
Country	The authentication factor is the country based on the IP address of the user computer.
Certificate Authentication	The certificate is used for authentication.
For the Day/Date/Time related conditions, you can choose between the user's local time and Universal Time Coordinated (UTC) time.	

7. Click the **Add** button associated with the filter and condition.
8. Select the profile you want applied if all filters/conditions are met in the **Authentication Profile** drop-down.

   The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the **Add New Profile** option. See "Creating Authentication Profiles" on page 284
9. Click **OK**.
10. (Optional) In the **Default Profile (used if no conditions matched)** drop-down, you can select a default profile to be applied if a user does not match any of the configured conditions.

    Note: If you have no authentication rules configured and you select **Not Allowed** in the **Default Profile** drop-down, users will not be able to log in to the service.
11. (Optional) If you have more than one authentication rule, you can drag and drop the rules to a new position in the list to control the order they are applied.
12. Click **Save**.

Assigning SSH Key Management Permissions

You can delegate permissions to additional users and roles to manage the SSH key. Additionally, these users must have the "Privilege Access Service User" rights to see the SSH Key tab. See "Admin Portal Administrative Rights" on page 277 for more information about this administrative right.

For each SSH key, you can add user management accounts and specify the following permissions:

- Delete – Delete the SSH key that is stored in Privileged Access Service.
- Edit – Edit the SSH key information only.
- Grant – Add user management accounts and assign permissions.
- Inherited From – The permissions a user has for SSH keys are inherited from the listed administrative right.
- Retrieve – Retrieve the SSH key.
- View – View the SSH key information only.

To add users and assign permission:

1. Click **Resources**> **SSH Keys**.
2. Select the relevant SSH key.
3. Click **Permissions**.
4. Click the **Add** button.
   a. Start typing the user, group, or role in which you want to assign SSH key management permissions.
   b. Select the relevant user, group, or role.
   c. Click **Add**.
   d. The user is added to the Permissions page with only View permission.

5. Assign the necessary permissions by selecting the relevant check-box.
6. Click **Save**

The user now has the specified permissions to manage this SSH key.

Adding Systems

If you want to manage accounts for a server, workstation, or network device through the Privileged Access Service, you must first add the computer or network device to the Systems list of servers. Initially, you might add systems and shared accounts one-by-one using the Add System Wizard, which guides you through the information required. Alternatively, you can create an import file to add multiple systems and shared accounts at once.

After you add or import the systems you want to manage, you can organize them into **system sets** to simplify other tasks such as assigning set-specific permissions, enabling a request and approval workflow, or configuring automatic account lockout managment.

For more information about performing these tasks, see the following topics:

- "Adding Systems with the Wizard" on the next page
- "Importing Systems and Accounts" on page 621
- "Adding System Sets" on page 536

Adding Systems with the Wizard

The **Add System** Wizard provides step-by-step guidance to help you add different types of systems one-by-one. The wizard prompts you to set the appropriate system properties based on the type of system you are adding and, optionally, attempts to verify the information you provide. You can change or add system information outside of the wizard at a later time, if needed. The following details how to:

Add a new system using the wizard

- "Add a new system using the wizard"
- "Choosing a system profile"

Add a New System Using the Wizard

1. In the Admin Portal, click **Resources**, then click **Systems** to display the list of computers and network devices.
2. Click **Add System** to open the **AddSystem** Wizard.
3. Enter the following information:
   - **System Type**: Select the system type from the drop-down menu. You can use the Delinea Admin Portal to manage account passwords for many types of systems. If you are adding a type of network device not available in the Admin Portal, select Generic SSH as the system type. If you would like to add a custom system type, see "Adding or managing a resource profile."
   - **DNS Name/IP Address**: Type the fully-qualified DNS name or IP address. FQDN is recommended for systems using a certificate to establish a trusted connection (usually HTTPS).
   - **Name**: Type a unique name to identify the system.
   - **Description**: (Optional) Type a description of the system.
4. Click **Next** to continue.
5. Optionally, add a user name and password (or SSH Key for some system types) for an account used to access the system and specify whether the password for the account is managed by the Privileged Access Service, then click **Next**.

   Some systems require a local administrative account to be specified if you want passwords managed by the Privileged Access Service. You can select **Make this account the local administrative account for this system** to designate the account you are adding as the local administrative account. You can also add or change the designated local administrative account after adding a system. For more information about identifying a local administrative account, see "Specifying a local administrative account."

   An account with an associated SSH key cannot be used as the local administrative account as there is no password stored for the account in the Privileged Access Service.

   Note that to set or change the local administrative account, you must have the **Edit** permission on the system and the **Grant** permission on the account. You have these permissions by default if you add the system and account to the Privileged Access Service.
6. For **Credential Type**, select **Password** or **SSHKey**. If choosing an SSH Key, you can either drag the key and drop it or click **Choose** and use a key on your computer. Additionally, you can click **Managethiscredential** if you wish to have the keys rotated.

7. Configure additional settings as appropriate, then click **Next**.

   The wizard prompts you for settings based on the type of system you are adding. For more information about system-specific settings, see the following topics:

   - "Adding Windows systems"
   - "Adding UNIX systems"
   - "Adding Cisco IOS or Cisco NX-OS systems"
   - "Adding Cisco AsyncOS systems"
   - "Adding Juniper systems"
   - "Adding HP NonStop systems"
   - "Adding IBM i systems"
   - "Adding Check Point Gaia systems"
   - "Adding Palo Alto Networks PAN-OS systems"
   - "Adding F5 Networks BIG-IP systems"
   - "Adding VMware VMkernel systems"
   - "Adding Generic SSH systems"

8. Select **Verify System Settings** to test access to the system using the account information provided, then click **Finish**.

   If the system and account settings are verified, click **Close**.

   If verification fails, try the following:

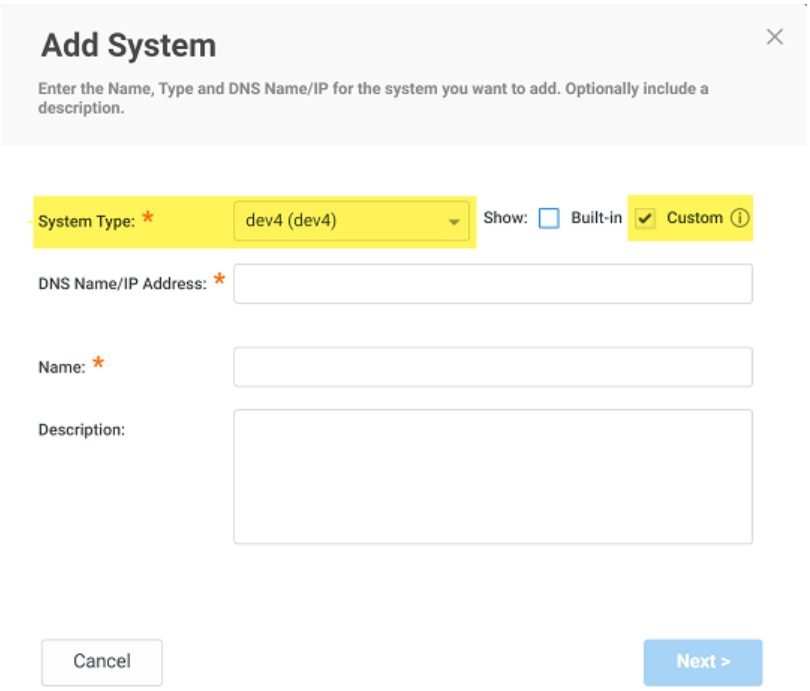
   - Test network connectivity.
   - Verify that the user name and password are valid.
   - Make sure you are using the latest version of the Delinea Connector.
   - Close the error message, deselect **Verify System Settings**, then click **Finish**.

   Note that you can only skip verification if the password for a system account is unmanaged. If you specify an account for a system and select **Manage this credential**, the connection to the system must be verified to ensure the correct password is stored by the Privileged Access Service.

Choosing a System Profile

Now that you have a new system, you can navigate to **Resources** > **Systems** and when you click **Add System** you can choose the system type you just created, enter a DNS Name/IP Address, a name, and an optional description.

Note: You can sort through system type to show custom types by clicking **Custom**.



Once you add the system, you can then add accounts and configure settings like normal. All operations going through the account are managed through the script that you "created."

Operations that you can perform may include but are not limited to the following:

- Login
- Checkout
- Update Password
- Rotate Password
- Set as an Admin Account
- Add to Set
- Verify Credential
- Delete
- Password Reconciliation

Adding Check Point Gaia Systems

If you are adding Check Point Gaia systems, you must install and start the SSH server on the target system before you can connect using Privileged Access Service. You can add a user name and password for an account to be used to access the system using a secure shell session when adding the system or at a later time.

For any account you add, you can choose whether you want the Privileged Access Service to manage the account password. If you select **Manage this credential**, the Privileged Access Service automatically changes the password immediately after the account and system are added and each time the account is checked in.

If you select **Manage this credential**, keep in mind that the Privileged Access Service can only manage passwords for privileged user accounts that have sufficient rights to configure and save settings. In addition, if there are any pending changes for other user accounts, those changes will be saved when the Privileged Access Service updates a managed password.

However, if a user or a session selects the configuration lock or runs the command to unlock the system database to make configuration changes, the Privileged Access Service will not rotate or update any passwords until the lock is restored. By default, this might result in a password update being delayed by up to five minutes. You should also avoid setting the configuration lock by running the lock database override command because it could result in a password change not being saved until the next time the system is rebooted, which will lock the managed account and prevent it from being used.

If you must take over a managed account to make configuration changes, you should use the less forceful lock database command to prevent the Privileged Access Service from attempting to rotate or change a managed password before making your changes.

For more information about password and system management for Check Point Gaia systems, see the following topics:

- "Password Complexity Rules" below
- "Using Expert Mode" below

Password Complexity Rules

All managed passwords generated by the Privileged Access Service consist of at least one upper case letter, one lower case letter, one number, and one special character regardless of the system type. For Check Point systems, the following additional password rules apply:

- The password length is 6 to 128 characters
- The password complexity policy states how many character classes should be included. For example, characters in the password are divided into upper case alphabetic (A-Z), lower case alphabetic (a-z), digits (0-9), and all other characters. Therefore, a password complexity value of 3 allows passwords like abc123! or abcDEF5, but not abcXYZ.
- The password can include special characters, but the first character cannot be an asterisk (*) or the user will not be able to log on to the operating system.

If the first character of the password for the expert mode user is an asterisk (*), a factory reset will be required. Therefore, the default password profile for Check Point Gaia systems does not include the asterisk (*) as a supported special character. If you clone the default profile or use another profile to create a custom password profile, you should be aware of the restrictions on special characters for the specific operating system you are using.

Using Expert Mode

There are two modes of operation for managing Check Point Gaia systems when you access the system through secure shell session. The default mode for running system-specific administrative tasks uses the clish shell environment. The second mode of operation is called the expert mode and runs in a bash shell environment. When running in the expert mode, you can perform administrative tasks that affect the underlying operating system.

To enter the expert mode, you enter the expert password. If you want to store and manage the password for the expert mode, you must specify a local administrative account for the system. The local administrative account must have the privileges that are required to manage the password for expert mode. For example, the administrative account must have the following features enabled: selfpasswd, expert, expert-password, and version.

The local administrative account you specify for a system should be a dedicated account that is used exclusively by the Privileged Access Service. You can have the password for both the local administrative account and expert mode managed by the Privileged Access Service to avoid password changes by other users who have administrative privileges.

If you want to store and manage the password for expert mode, there are restrictions on the actions available for both the expert mode password and the local administrative account that has access to the expert mode. For example, you cannot select the **Login** action for the expert mode password because that action could be used to compromise the login shell for the local administrative account. Similarly, because the local administrative account is used internally to provide access to the expert mode password, you cannot select the Login, Checkout, Rotate Password, or Delete actions when you select an account currently designed as the local administrative account on a Check Point Gaia system.

Adding Cisco AsyncOS Systems

Overview

To manage Cisco AsyncOS system accounts, you need to specify a valid local administrative account and password. See "Specifying a local administrative account" for more information. The account used must be an account in the Cisco AsyncOS Administrator role.

To create a Cisco AsyncOS account in the Administrator role using the CLI or GUI, see the following:

- https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/cli_reference_guide/b_CLI_Reference_Guide.html
- https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide/b_ESA_Admin_Guide_ces_11_0/b_ESA_Admin_Guide_chapter_0100000.html

> **Note:** Since user accounts in the the Cisco AsyncOS Help Desk User role and the Custom user role are restricted from connecting to Cisco AsyncOS systems through SSH, those users, if added to Privileged Access Service, cannot use the Privileged Access Service login functions to connect to a Cisco AsyncOS system.

For any account you add, you can choose whether or not you want the Privileged Access Service to manage the account password. If you select **Manage this credential**, the Privileged Access Service automatically resets the password immediately after the account and system are added and each time the account is checked in.

You should also keep in mind that only the Privileged Access Service will know the managed password being generated and stored. You should not select this option if you don't want the Privileged Access Service to manage the password for the account.

For more information about password and system management for Cisco AsyncOS systems, see the following topics:

Password Complexity Rules

All managed passwords generated by the Privileged Access Service consist of at least one upper case letter, one lower case letter, one number, one special character, and allow consecutive repeated characters regardless of the system type. In the **Admin Portal > Settings > **Resources > Password Profiles**, the default password profile for Cisco AsyncOS systems restricts password length to a maximum of 32 characters. The following additional password rules apply:

- Minimum password length: 12 characters.
- Maximum password length: 32 characters.
- Supported special characters: ~ ? ! @ # $ % ^ & * - _ + = \ | / [] () <> {} ; : , .

You should keep in mind that only Privileged Access Service will know the managed password being generated and stored. You should not select this option if you don't want Privileged Access Service to manage the password for the account.

For information on changing system settings, see:

"Changing Cisco AsyncOS System Settings" below

Changing Cisco AsyncOS System Settings

You can use the System Settings to update the following types of information after adding a system:

- Session type or port number for remote connections

RDP is not supported for Cisco AsyncOS, therefore you should not change the session type. If you don't specify a session type and port, the secure shell client and port 22 are used by default.

- Select a system time zone

You can manually select the time zone you want to use for any system. If you don't specify a time zone, the local time zone of the system is used by default.

Adding Cisco IOS or NX-OS Systems

Overview

If you are adding a Cisco IOS or Cisco NX-OS system, you can add a user name and password for an account to be used to access the system when adding the system or at a later time.

You can specify any valid local user account and password. In most cases, however, you would specify admin or an account with similar privileges for which you want to manage the password. Only local accounts that can change their own passwords are supported.

For any account you add, you can choose whether or not you want the Privileged Access Service to manage the account password. If you select **Manage this credential**, the Privileged Access Service automatically resets the password immediately after the account and system are added and each time the account is checked in.

If you select **Manage this credential** for Cisco IOS and NX-OS devices, you should keep in mind that the Privileged Access Service can only manage passwords for privileged user accounts that have sufficient rights to configure and save settings. In addition, if there are any pending changes for other user accounts, those changes will be saved when the Privileged Access Service updates a managed password.

You should also keep in mind that only the Privileged Access Service will know the managed password being generated and stored. You should not select this option if you don't want the Privileged Access Service to manage the password for the account.

For more information about password and system management for Cisco systems, see the following topics:

- "Password Complexity Rules" below
- "Changing Cisco IOS or NX-OS System Settings" below

Password Complexity Rules

All managed passwords generated by the Privileged Access Service consist of at least one upper case letter, one lower case letter, one number, and one special character regardless of the system type. For Cisco NX-OS systems, the following additional password rules apply:

- Minimum password length: 12 characters.
- Maximum password length: 32 characters.
- Supported special characters: !@#%&()*+,-./:;<>[]^_{|}~

For Cisco IOS systems, the following additional password rules apply:

- Minimum password length: 12 characters.
- Maximum password length: 25 characters.
- Supported special characters: !@#$%&()*+,-./:;<=>[]^_{|}~

Changing Cisco IOS or NX-OS System Settings

You can use the System Settings to update the following types of information after adding a system:

- Change the session type or port number for remote connections.

  You can manually select secure shell or remote desktop and change the port number for remote sessions. If you don't specify a session type and port, the secure shell client and port 22 are used by default.

- Select a system time zone.

  You can manually select the time zone you want to use for any system. If you don't specify a time zone, the local time zone of the system is used by default.

- Add or modify the optional description of the system.

Adding F5 Networks BIG-IP Systems

Overview

To manage F5 Networks BIG-IP accounts, you need to specify a valid local administrative account and password. See "Specifying a local administrative account" for more information. The account used must be an account in the F5 Networks BIG-IP Administrator role.

To manage the password of other users and root accounts, the administrative account must have the F5 Networks BIG-IP role Administrator. Although users with the User Manager role can change passwords for users that do not have the Administrator role, it cannot change the password for users in the Administrator role.

For additional information, see: https://www.f5.com/.

For any account you add, you can also choose whether or not you want Privileged Access Service to manage the account password. If you select **Manage this credential**, Privileged Access Service automatically resets the password after the account and system are added and each time the account is checked in.

For more information on managing F5 Networks BIG-IP systems, see the following topics:

Setting up Certificates for F5 Networks BIG-IP Systems

You must set up the device certificate on the F5 Networks BIG-IP system before you can connect using Privileged Access Service.

Once the F5 Networks BIG-IP system is configured, the same certificate must also be trusted in all Delinea Connector systems that are connected to the F5 Networks BIG-IP system. In most cases, F5 Networks BIG-IP systems should use a certificate obtained from an Enterprise Certificate Authority (CA), or a trusted external CA, like VeriSign. Since the certificate is trusted already, it simplifies the certificate setup on Delinea Connector systems. You can also export the certificate from the F5 Networks BIG-IP system and import it into all systems running the Delinea Connector. Self-signed certificates should not be used in production environments.

Verifying Certificate Configuration

To verify that the certificate is trusted in the Delinea Connector, connect to the F5 Networks BIG-IP Web UI ("`https://<hostname/IP Address>:<management port>`") using a browser and verify that the connection is secure. If the connection is secure, the SSL/TLS secure management channel is established.

If an error occurs while establishing the SSL connection, review the supported SSL/TLS protocol versions and cipher suites.

If an error occurs indicating that the server certificate cannot be validated, check the connector and target certificate settings, including root CA, subject names, and validity.

For more information about password and system management for F5 Networks BIG-IP systems, see the following topics:

- "Adding F5 Networks BIG-IP Systems" on the previous page
  - "Overview" on the previous page
  - "Setting up Certificates for F5 Networks BIG-IP Systems" on the previous page
    - "Verifying Certificate Configuration" on the previous page
  - "Password Complexity Rules" below
  - "Changing F5 Networks BIG-IP System Settings" below

Password Complexity Rules

All managed passwords generated by the Privileged Access Service consist of at least one upper case letter, one lower case letter, one number, one special character, and allow consecutive repeated characters regardless of the system type. In the **Admin Portal > Settings >Resources>Password Profiles**, the default password profile for F5 Networks BIG-IP restricts password length to a maximum of 31 characters. The following additional password rules apply:

- Minimum password length: 12 characters.
- Maximum password length: 31 characters.
- Supported special characters: @#%*+,-./:=?[]^_~

Note: You should not use the following special characters in passwords that you define for F5 Networks BIG-IP user accounts: ( ) ; ! | $ < > & ' " ` \ { }

You should keep in mind that only Privileged Access Service will know the managed password being generated and stored. You should not select this option if you don't want Privileged Access Service to manage the password for the account.

For additional information on F5 Networks BIG-IP system password requirements, see the following reference:

https://support.f5.com/csp/article/K2873

Changing F5 Networks BIG-IP System Settings

In addition to the common system settings you can change for any type of system, there are a few F5 Networks BIG-IP system settings. For example, you can use System Settings to update the following types of information after adding a system:

- Change the session type or port number for remote connections

You can manually select secure shell or remote desktop and change the port number for remote sessions. If you don't specify a session type and port, the secure shell client and port 22 are used by default.

- Select a system time zone

You can manually select the time zone you want to use for any system. If you don't specify a time zone, the local time zone of the system is used by default.

- Account Management Settings

For password management, HTTPS port 8443 is used. If you changed the port assignment used for password management, you need to manually set the Management Port field to match the setting of the F5 Network BIG-IP system. Contact F5 Networks BIG-IP Support if you want to change the port setting.

Adding Generic SSH Systems

Overview

If you are adding a Generic SSH system, you can add a user name and password or a SSH key for an account to be used to access the system using a secure shell session. See "Adding SSH keys" on page 512 for information on adding SSH keys to Privileged Access Service.

You cannot use Privileged Access Service to manage account passwords for generic SSH systems. However, you can use Privileged Access Service to store the account information securely, then use the account to open secure shell sessions on target systems without knowing the password.

You can specify any valid local user account and password. In most cases, however, you would specify root or an account with similar privileges for which you want to manage the password.

Changing Generic SSH System Settings

If you set the system-specific or global policy to allow remote access from a public network and the system is a network device that supports secure shell (SSH) connections, you can use the System Settings to select **SSH** as the session type and specify the port number to use for secure shell sessions.

In the Settings page, you can set a domain for a system and then enable domain operations to use the domain administrative account to enable zone role workflow. For configuration steps, see "Setting Domain Operations for a System" on page 556

You can also use System Settings to specify a time zone or to add or modify the optional description of the device.

Adding HP NonStop Systems

Overview

If you are adding HP NonStop Guardian systems, be sure that the Safeguard and SSH components are installed on the hardware. If these components are installed, you can add a user name and password for an account to be used to access the system when adding the system or at a later time.

User names in Guardian are of the form group-name.user-name, for example acme.harvey is a user name in a group called acme. User IDs in Guardian are in the form group-id,user-id. For example if the acme group has a Group ID of 154 and harvey has a User ID of 1 within that group, the User ID of acme.harvey is 154,1.

In most cases, however, you would specify the SUPER.SUPER (255,255) account, a group manager account, or an account with similar privileges for which you want to manage the password. For example, user 154,255 would be the group manager account in acme group.

Each Guardian user account can have multiple aliases that share the same Guardian User ID and the same access permissions to system systems, but cannot use the same password as each other or use the same password as the Guardian User ID they are based on. Aliases can also be managed separately from their underlying User ID. For example, you might want to set up an alias user for SUPER.SUPER so that each NonStop administrator has the same permissions as SUPER.SUPER, but each one maintains their own password.

For any account you add, you can choose whether or not you want the Privileged Access Service to manage the account password. If you select **Manage this credential**, the Privileged Access Service automatically changes the password immediately after the account and system are added and each time the account is checked in.

If you select **Manage this credential** for HP NonStop devices, you should keep in mind that the Privileged Access Service can only manage passwords for privileged user accounts that have sufficient rights to configure and save settings. In addition, if there are any pending changes for other user accounts, those changes will be saved when the Privileged Access Service updates a managed password.

For more information about password and system management for HP NonStop systems, see the following topics:

- "Password Complexity Rules" below
- "Specifying Proxy Users for SUPER.SUPER" below

Password Complexity Rules

All managed passwords generated by the Privileged Access Service consist of at least one upper case letter, one lower case letter, one number, and one special character regardless of the system type. For HP NonStop systems, the following additional password rules apply:

- Minimum password length: 8
- Maximum password length: 8
- Supported special characters: !@#%&()*+-./:<>[]^_{|}~

The default password profile for HP NonStop systems will only include supported special characters. If you clone the profile to create a custom password profile, you should be aware that on some versions of the operating system, some special characters are not supported and should not be used in the password. For example, on some versions of the HP NonStop operating system, you should avoid adding the following special characters to the profile: , ; “” $ =

For more information, see the HP Security Management Guide: http://h20565.www2.hpe.com/hpsc/doc/public/display?sp4ts.oid=4201303&docLocale=en_US&docId=emr_na-c02131793

Specifying Proxy Users for SUPER.SUPER

If you selected HP NonStop as the system type and added SUPER.SUPER as the account to use with the device, you are prompted to specify whether the SUPER.SUPER user account is allowed to log on using secure shell (ssh) connections.

Adding IBM i Systems

Overview

If you are adding IBM i systems, you must install and start the SSH server on the target system before you can connect using Privileged Access Service.

Accounts on IBM i are called profiles. For example, you can specify the user profile QSECOFR as the account used to access the system. This is the most powerful user profile, and is similar to root on UNIX. The use of a proxy account and password is not supported on IBM i.

For any user profile (account) you add, you can choose whether you want the Privileged Access Service to manage the account password. If you select **Manage this credential**, the Privileged Access Service automatically changes the password immediately after the account and system are added and each time the account is checked in for each password profile associated with the account.

If you select **Manage this credential** for IBM i devices, keep in mind that the Privileged Access Service can only manage passwords for privileged user accounts that have sufficient rights to configure and save settings. In addition, if there are any pending changes for other user accounts, those changes will be saved when the Privileged Access Service updates a managed password.

For more information about password and system management for IBM i systems, see the following topic:

"Password Complexity Rules" below

Password Complexity Rules

All managed passwords generated by the Privileged Access Service consist of at least one upper case letter, one lower case letter, one number, and one special character regardless of the system type. For IBM i systems, the following additional password rules apply:

- On IBM i, the password complexity is affected by system settings, especially the password level, QPWDLVL. Administrators select the password level based on interoperability requirements for the system.
- A password level of 0 or 1 restricts the password length to 10 characters. Supports special characters are $, @, #, and underscore.
- A password level of 2 or 3 supports up to 128 characters. All characters are supported, except that the password must not begin with an asterisk (*). These password levels allow the use of a passphrase with internal blanks (spaces) between words. Trailing blanks are ignored. The password is case-sensitive.

The default password profile for IBM i systems will only include supported special characters. You can clone the default password profile to modify its settings. For example, with a custom password profile you could set the password to allow more than 10 characters when running QPWDLVL 2 or 3.

If you clone the default or another system password profile to create a custom password profile, however, you should be aware that on some versions of the operating system, some special characters might not be supported and should not be used in the password. You can also create a custom profile.

Additional IBM i system settings also impact the maximum password length and other password rules.

- QPWDCHGBLK: Block password change
- QPWDEXPITV: Expiration interval
- QPWDEXPWRN: Password expiration warning
- QPWDLMTCHR: Restricted characters
- QPWDLMTAJC: Restrict adjacent characters
- QPWDLMTREP: Restrict repeating characters
- QPWDMINLEN: Minimum length
- QPWDMAXLEN: Maximum length
- QPWDPOSDIF: Character position difference

- QPWDRQDDIF: Required difference
- QPWDRQDDGT: Require numeric character
- QPWDRULES: Password rules
- QPWDVLDPGM: Password validation program

For more information about managing user passwords, see “System values that apply to passwords in the IBM System i Security Reference” for the appropriate IBM i release:

- "6.1: https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_61/rzarl/sc415302.pdf"
- "7.1: https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_71/rzarl/sc415302.pdf"

Adding Juniper Systems

Overview

If you are adding a Juniper Junos OS system, you can add a user name and password for an account to be used to access the system when adding the system or at a later time.

You can specify any valid local user account and password. In most cases, however, you would specify admin or an account with similar privileges for which you want to manage the password.

For any account you add, you can choose whether or not you want the Privileged Access Service to manage the account password. If you select **Manage this credential**, the Privileged Access Service automatically resets the password immediately after the account and system are added and each time the account is checked in.

If you select **Manage this credential** for Juniper Junos OS devices, you should keep in mind that the Privileged Access Service can only manage passwords for privileged user accounts that have sufficient rights to configure and save settings. In addition, if there are any pending changes for other user accounts, those changes will be saved when the Privileged Access Service updates a managed password.

You should also keep in mind that only the Privileged Access Service will know the managed password being generated and stored. You should not select this option if you don’t want the Privileged Access Service to manage the password for the account.

For more information about password and system management for Juniper systems, see the following topics:

- "Password Complexity Rules" below
- "Specifying Proxy Users for Root" on the next page
- "Changing Juniper System Settings" on the next page

Password Complexity Rules

All managed passwords generated by the Privileged Access Service consist of at least one upper case letter, one lower case letter, one number, and one special character regardless of the system type. For Juniper Junos OS systems, the following additional password rules apply:

- Minimum password length: 12 characters.
- Maximum password length: 20 characters.
- Supported special characters: !@#$%&()*+,-./:;<=>?[]^_{|}~

Specifying Proxy Users for Root

If you selected Juniper as the system type and added root as the account to use with the device, you are prompted to specify whether the root user account is allowed to log on using secure shell (ssh) connections.

You can disable secure shell (ssh) connections for root on Juniper devices by running the following command:

```
set system services ssh root-login deny
```

If you have disabled secure shell (ssh) connections for root and want to manage the password for the account, you must add a user name and password for an account that can open a secure shell connection on the target system.

The account name and password you specify becomes a “proxy” account used in place of the root account. The account used as the “proxy” for the root account must be able to open secure shell sessions on the target system, but no other special privileges are required. After the “proxy” account opens the secure shell connection, it gets its root privileges programmatically to perform administrative tasks on the target system.

If you are adding a “proxy” account to open secure shell sessions, you also have the option to have the password for this account managed by the Privileged Access Service. If you select **Manage this credential** for the proxy account, only the Privileged Access Service will know the password for the account from this point on. The managed password for the “proxy” account will not be available to any other applications or users.

Changing Juniper System Settings

You can use the System Settings to update the following types of information after adding a system:

- Select a system time zone.

  You can manually select the time zone you want to use for any system. If you don’t specify a time zone, the local time zone of the system is used by default.
- Change proxy account settings.

  If you configure ssh to prevent the root user account from logging on using secure shell connections, you can select the **Enable Proxy Account** option to set the proxy user name and password.
- Add or modify the optional description of the system.

Adding Palo Alto Networks PAN-OS Systems

Overview

To manage Palo Alto Networks PAN-OS accounts, you need to specify a valid local administrative account and password. See "Specifying Local Admin Accounts" on page 565 for more information. The account used must be a superuser account.

For any account you add, you can also choose whether or not you want the Privileged Access Service to manage the account password. If you select **Manage this credential**, the Privileged Access Service automatically resets the password after the account and system are added and each time the account is checked in.

Note: If you select **Manage this credential** for Palo Alto Networks PAN-OS systems, keep in mind that the Privileged Access Service can only manage passwords for administrator accounts with local authentication (password). Accounts with an authentication profile set (including local user databases) are not supported.

For more information about password and system management for Palo Alto Networks PAN-OS systems, see the following topics:

- "Setting up Certificates for Palo Alto Networks PAN-OS Systems" below
- "Password Complexity Rules" on the next page
- "Changing Palo Alto Networks PAN-OS System Settings" on the next page

Setting up Certificates for Palo Alto Networks PAN-OS Systems

You must set up the certificate and SSL/TLS Service Profile on the PAN-OS system before you can connect using Privileged Access Service.

For configuration information, see the *PAN-OS Web Interface Reference* and the *PAN-OS Admin Guide*:

https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-certificate-management-ssltls-service-profile

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/certificate-management/replace-the-certificate-for-inbound-management-traffic

Once the PAN-OS system is configured, the same certificate must also be trusted in all connector systems that are connected to the PAN-OS system. In most cases, PAN-OS systems should use a certificate obtained from an Enterprise Certificate Authority (CA), or a trusted external CA, like VeriSign. Since the certificate is trusted already, it simplifies the certificate setup on connector systems. You can also export the certificate from the PAN-OS system and import it into all systems running the connector. Self-signed certificates should not be used in production environments.

Note: Palo Alto Networks PAN-OS system accounts are managed using an API via HTTPS. A secure channel is required between the connector and the Palo Alto Networks PAN-OS system. Certificates are typically issued to a fully qualified domain name (FQDN). Therefore, if an IP address is provided instead, the server certificate may not be validated.

Verifying Certificate Configuration

To verify that the certificate is trusted in the connector, connect to the PAN-OS Web UI ("https://<PAN-OS hostname/IP Address>") using a browser and verify that the connection is secure. If the connection is secure, the SSL/TLS secure management channel is established.

- If an error occurs while establishing the SSL connection, review the supported SSL/TLS protocol versions and cipher suites.
- If an error occurs indicating that the server certificate cannot be validated, check the connector and target certificate settings, including root CA, subject names, and validity.

For more information about password and system management for Palo Alto Networks PAN-OS systems, see the following topics:

- "Password Complexity Rules" below
- "Changing Palo Alto Networks PAN-OS System Settings" below

Password Complexity Rules

All managed passwords generated by the Privileged Access Service consist of at least one upper case letter, one lower case letter, one number, one special character, and allow consecutive repeated characters regardless of the system type. Palo Alto Networks PAN-OS systems, restrict passwords to a maximum of 31 characters. The following additional password rules apply:

- Minimum password length: 12 characters.
- Maximum password length: 31 characters.
- Supported special characters: !$%&()*+,-./:;<=>?[]^_{|}~

You should keep in mind that only the Privileged Access Service will know the managed password being generated and stored. You should not select this option if you don't want the Privileged Access Service to manage the password for the account.

For additional information on Palo Alto Networks PAN-OS system password requirements, see the *PAN-OS Web Interface Reference*:

https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-password-profiles/username-and-password-requirements

Changing Palo Alto Networks PAN-OS System Settings

In addition to the common system settings you can change for any type of system, there are a few Palo-Alto Networks PAN-OS system settings. For example, you can use System Settings to update the following types of information after adding a system:

- Change the session type or port number for remote connections

  You can manually select secure shell or remote desktop and change the port number for remote sessions. If you don't specify a session type and port, the secure shell client and port 22 are used by default.

- Select a system time zone

  You can manually select the time zone you want to use for any system. If you don't specify a time zone, the local time zone of the system is used by default.

- Account Management Settings

  For password management, port 443 is used. If you changed the port assignment used for password management, you need to manually set the Management Port field to match the setting of the PAN-OS system. Contact Palo Alto Networks Support if you want to change the port setting.

Adding System Accounts

In most cases, you add at least one account for accessing a system when you initially add the system to Privileged Access Service. If you did not add an account when you added or imported a system, provided invalid account information when you added the system, or want to update the system to include additional accounts, you can do so after adding a system by clicking **Accounts** when viewing the details for the system.

To add a new account for a specific system:

1. In the Admin Portal, click **Resources**, then click **Systems** to display the list of computers and network devices.
2. Select a Unix system to display system-specific details.
3. Ensure the **Accounts** tab is open and click the **Add** button.
4. Type the user name for an account you want to use to access the currently selected system.
5. Use the **Credential Type** drop down list to choose how you want the user to access this system (Password or SSH Key).
   a. If you select **Password**, enter the password you want associated with this account.
   b. If you select **SSH Key**, select **Upload or Choose** using the toggle button.
      - **Choose** allows you to choose an SSH key from a file on you have already added to Privileged Access Service.
      - **Upload** allows you to drag and drop the SSH key from a file on your desktop or click in the drop area to select an SSH key from a file location.
6. (Optional) Select the **Manage this credential** option if you want Privileged Access Service to manage the password for the specified account. For details about managed passwords for different types of systems, see the following sections:
   - "Adding Windows Systems" on page 545
   - "Adding UNIX Systems" on the next page
   - "Adding Cisco IOS or NX-OS Systems" on page 524
   - "Adding Cisco AsyncOS Systems" on page 523
   - "Adding Juniper Systems" on page 531
   - "Adding HP NonStop Systems" on page 528
   - "Adding IBM i Systems" on page 529
   - "Adding Check Point Gaia Systems" on page 521
   - "Adding Palo Alto Networks PAN-OS Systems" on page 532
   - "Adding F5 Networks BIG-IP Systems" on page 526
   - "Adding VMware VMkernel Systems" on page 544
   - "Adding Generic SSH Systems" on page 528
7. Optionally, type a description for the account, then click **Add**.
8. Click **Save** to save the new account for the system.

The information displayed and the actions you can take after clicking Accounts are the same whether you navigate to them from the system details or from the full list of accounts.

For example, if you are viewing the accounts for a specific system, you can also select any account in the list, then click the Actions menu to perform account-related tasks. The steps for completing any action are the same regardless of how you navigate to them. For more information about performing these common tasks, see "Selecting System Actions" on page 470

Adding System Sets

After you have added systems, you can organize them into logical groups—system sets—to simplify management activity and reporting for systems with attributes in common.

To add a system set:

1. In the Admin Portal, click **Resources**, then click **Systems** to display the list of computers and network devices.
2. In the Sets section, click **Add** to create a new set.
3. Type a name for the new set, an optional description, and select whether group membership is manual or dynamic.

   For manual sets, you can specify permissions for both the set itself and the members of the set. For dynamic sets, you can only specify permissions on the set.
4. Identify the members of the set in one of two ways.
   - If set membership is **Dynamic**, type the SQL statement to execute to identify set members in the **Query** field. For example, if you want to add a set for the systems with a name that starts with mem, you could type a SQL statement like this:

     ```
     select id from server where name like 'mem%'
     ```

   - If you select **Manual**, click **Members**, then click **Add** to search for and select the systems to add as members.
5. Click **Save**.

Adding UNIX Systems

For UNIX systems, you can specify any valid local user account with a password or SSH key. When using a password for that account, however, you would likely specify root or an account with similar privileges for which you want to manage the password. If you want to use a SSH key for that account, you must have a key uploaded to Privileged Access Service. See "Adding SSH keys" on page 512

If you have added an account with a password, you can also choose to have Privileged Access Service manage the account password. Password management means that Privileged Access Service automatically resets the password after the account and system are added and each time the account is checked in. See "Adding System Accounts" on page 534 for information about configuring password management.

Password Complexity Rules

All managed passwords generated by the Privileged Access Service consist of at least one upper case letter, one lower case letter, one number, and one special character regardless of the system type. For UNIX systems, the following additional password rules apply:

- Minimum password length: 12 characters.
- Maximum password length: 32 characters.
- Supported special characters: !$%&()*+,-./:;<=>?[]^_{|}~

You should keep in mind that only the Privileged Access Service will know the managed password being generated and stored. You should not select this option if you don't want the Privileged Access Service to manage the password for the account.

Specifying Proxy Root Accounts

The most common scenario for most UNIX systems is to have the Privileged Access Service manage the password for the local root user. However, it is also very common to configure secure shell environments to prevent the root user from opening secure shell connections, which would prevent the account from being used to log on to target systems.

To address these two common scenarios, the Privileged Access Service allows you to specify a "proxy" account to use in place of the root account. The "proxy" account is used to open the secure shell session on the target system. The account used as the "proxy" for the root account does not require any special privileges. The only requirement for the "proxy" account is that it must be allowed to open secure shell sessions on the target system. After the "proxy" account opens the secure shell connection, the Privileged Access Service gets root privileges programmatically, enabling the account to perform administrative tasks on the target system.

Note: Accounts using SSH key as the credential type cannot have a proxy account.

Checking If a Proxy Account is Required

If you have configured SSH to prevent the root user account from logging on using secure shell (SSH) connections, you must add a user name and password for an account that can open a secure shell connection on the target system. If necessary, you can open the /etc/ssh/sshd_config file on the server to verify whether the PermitRootLogin parameter is set to no. If the PermitRootLogin parameter is set to no, you must specify a "proxy" account.

Managing Passwords for Proxy Accounts

If you are using a "proxy" account as a substitute for the root user account, you also have the option to have the password for the "proxy" account managed by the Privileged Access Service. If you select **Manage this credential** for a "proxy" account, only the Privileged Access Service will know the password for the account. The managed password for the "proxy" account will not be available to any other applications or users.

You can specify the proxy account information when adding the system using the Add System wizard or an import template or after you have added the system using the System Settings.

Configuring UNIX Local Account Reconciliation

You can reset out-of-sync managed local UNIX and Linux account passwords stored in Privileged Access Service using the following methods:

- Delinea Client for Linux
- Local administrative account
- Provisioning administrative account

If desired, you can configure local account reconciliation to use the client and then use either the local or domain administrative account as a backup method. If you do that, be sure to follow the procedures for both configurations.

When a password change operation of an account fails, Delinea PAS retries the change operation periodically. If Local Account Reconciliation is enabled on the system, then Delinea PAS also reconciles the password as part of the password change operation. A password reset of local managed accounts is initiated if an out-of-sync password is detected during account login, account checkout, and rotate operations.

All events are logged and can be viewed in the Admin Portal **Resources> Systems > Activity** page. You can also build custom reports to view activity, see "How to Create a New Report" on page 1055

Note: If you configure password reconciliation using both the client and a local administrative account, Delinea PAS attempts to use the client method first. If Delinea PAS encounters a connection issue using the client, it will then use the local administrative account to reconcile the out-of-sync password.

This topic includes the following sections:

Using the Delinea Client for Linux for Account Reconciliation

Before you configure local account password reconciliation for Linux systems using the Delinea Client for Linux, make sure that the local and service user accounts that are allowed to access the stored and managed account passwords have the Agent Auth permission.

For installation information, see "Enrolling and Managing Computers Using the Cloud Client for Linux" on page 53

To configure local account password reconciliation on systems with the Delinea Client for Linux installed:

1. In the Admin Portal, navigate to **Resources > Systems** and then select the system where you want to enable password reconciliation.
2. Click **Client Profile** to view the client details and make sure that the system has the client installed and enrolled.
3. Click **Advanced** and in the **Account Reconciliation Settings** area, select **Yes** next to **Local Account Automatic Maintenance**, to enable the policy to automatically manage the passwords for local system accounts.

   Note: You do not need to set a local administrative account (**Account Reconciliation > Local Administrative Account**) for systems that have the Delinea Client for Linux installed. If you do configure the local administrative account, Delinea PAS will only use the local administrative account to reconcile the out-of-sync password if it encounters a connection issue using the client. See "Configuring a system to use a local administrator for local UNIX account reconciliation "for configuration details.
4. Click **Save**.

Using Local Administrators for Local UNIX Account Reconciliation

Before you configure local account password reconciliation for UNIX systems, make sure the following requirements have been met:

- You must know the password of the account you are storing as a local administrative account.
- The user to be configured as the administrative account needs to be a root user or a user with sudo privileges to run the passwd command.

- Both the administrator account and the user account that requires a password change are required to use a password and not an SSH key.
- There must be a connector that can connect to this UNIX system.
- Your account must have the **Edit** permission for the system in order to configure the settings in the following procedure.

The Privileged Access Service can manage local administrative accounts but cannot reconcile local administrative account passwords that are out of sync. If the local administrator account encounters an issue, operations using the local administrative account will fail. See the account Activity page for error details.

To configure local account password reconciliation on UNIX systems using a local administrative account:

1. If the system already exists in the Admin Portal, click **Resources> Systems** to display a list of systems.

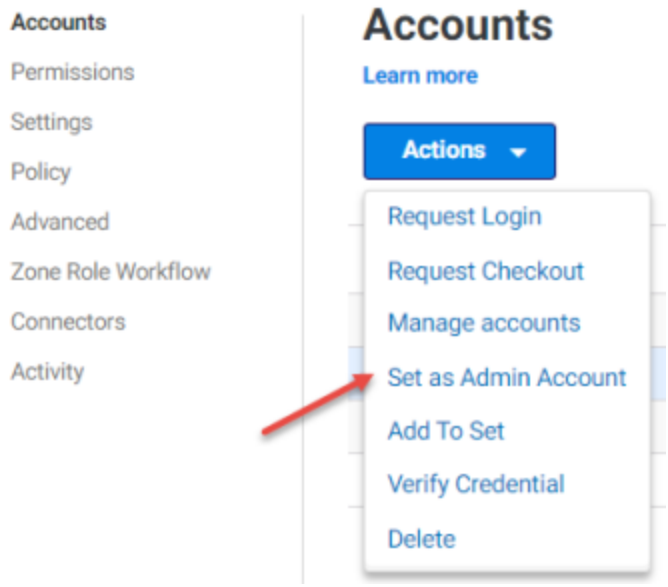
   Discovered systems, synced systems (with an active connector) and manually added systems are displayed.

   > **Note:** If you are adding a new UNIX system, you can add a local administrator account as part of the Add System process, see "Adding Systems with the Wizard" on page 519

2. Select the system where you want to add an administrative account, and then click the **Advanced** page.
3. Specify which account to use as the local administrative account:
4. - In the Administrative Account Settings area, next to **Local Administrative Account**, click **Set**. Then, in the **Select Account** text box start typing the name of the account you want to be the local administrator account and then click **Select**.

     > **Note:** The Provision button next to Local Administrative Account works if you've configured a Provisioning Administrative Account. For details, see "Configuring Domains with a Provisioning Admin Account for Local UNIX Account Reconciliation" on page 541

   - You can alternatively set up an administrative account for a UNIX system in the Systems > Account page. Click **Resources> Systems** and select the system where you want to add an administrative account. Select the **Accounts** page and then select the account you want to be the local administrative account. Selecting an account activates the Actions menu. From the Actions menu, select **Set as Admin Account**.



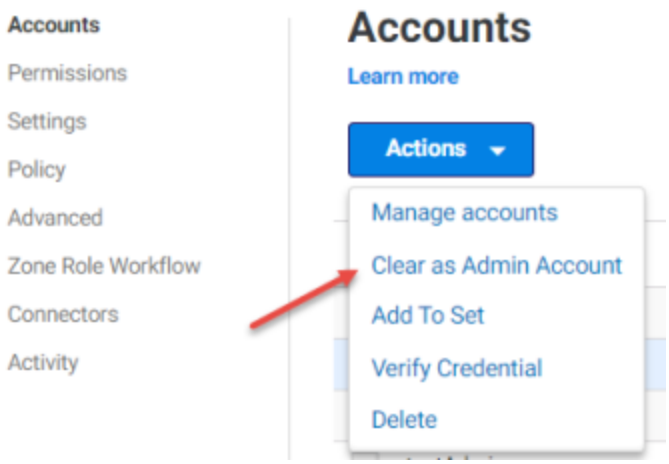
5. After specifying a local administrative account, in the **Account Reconciliation Settings** area, for the **Local Account Automatic Maintenance**, select **Yes** to to manage the passwords automatically for local system accounts.
6. Click **Save**.

   Delinea PAS will now use the specified local administrative account to manage passwords for local accounts on this system.

To clear a local administrative account

1. In the Admin Portal, click **Resources> Systems** to display a list of systems.
2. Select the desired system.
3. In the Accounts page, check the box next to the administrative account you want to clear.

   Selecting an account activates the **Actions** menu.
4. From the Actions menu, select **Clear as Admin Account**.



You can also clear the administrative account from the **Resources> Systems > Advanced** page.

Configuring Domains with a Provisioning Admin Account for Local UNIX Account Reconciliation

As a more secure alternative to using a domain administrative account, you can configure a *provisioning administrative account* to handle the local account password reconciliation on UNIX systems. The provisioning administrative account is a managed account that creates a local administrative service account (called the *reconciliation account*) that handles the password reconciliation on UNIX systems. Directly after creating the reconciliation account, the service rotates the password of the provisioning administrative account.

Delinea PAS performs all password rotations on the affected systems using the reconciliation account. If the password change fails because the password is out of sync, an event is created, and a hard password reset is done. Local account password reconciliation (LAPR) is only available for managed local accounts on domain-joined UNIX systems.

Note: The Management Mode and Proxy settings configured for a system (located in **Admin Portal** > **Resources** > **Systems** > **Settings**) do not apply if local account password reconciliation is enabled. For management mode, the system defaults to SMB when password reconciliation is configured. If reconciliation is not enabled for a system using the Delinea Connector, then management mode and proxy account settings are used for managed accounts.

Here are the prerequisites for configuring a provisioning administrative account for a UNIX system:

- The UNIX system need to be joined to a domain
- A connector needs to be able to reach the UNIX system
- The account you want to specify as a provisioning administrative account must:
  - Be a managed account (in the Domain > Accounts list)
  - Have sudo permission to run sh and to create the reconciliation account and grant it with sudo permissions

After the provisioning administrative account creates the local reconciliation account, Delinea PAS rotates the provisioning administrative account password automatically.

Here are some things to know about the reconciliation account:

- Delinea PAS creates the account on the UNIX system and the account has the name specified in the Reconciliation Account Name field.
- The reconciliation account is a local administrative account on the UNIX system.
- Delinea PAS manages the password for the reconciliation account. DelineaDelinea
- The reconciliation account does not appear in the list of system accounts. Delinea PAS lists the account in the Local Service Accounts set, which you can either see on the system's Advanced page or by going to Resources > Accounts > Sets. Delinea
- If you delete the reconciliation account in Centrify PAS, the service also removes the account from the UNIX system (unless the delete prompt explicitly states otherwise).

You first configure settings on the domain, and then on the individual system.

To configure a provisioning account on the domain for local account password reconciliation

Note: The user logged in to the Admin Portal must have the **Edit** permission for the domain to configure the account reconciliation settings described in this procedure.

1. In the Admin Portal, click **Resources>Domains** to display a list of domains.
2. Select the domain and then click the **Advanced** page.
3. In the UNIX/Linux Local Accounts area, for the Provisioning Administrative Account, click Set.

   The Select Account dialog opens.
4. Search for and select the desired account, then click **Select**.

   The specified account now is added as the Provisioning Administrative Account.
5. In the **Reconciliation Account Name** field, enter the name that you want the account to appear as in the UNIX systems.
6. Click **Save**.

   The Provisioning Administrative Account will now display for UNIX systems.

To provision a local administrative account on a UNIX system for local account password reconciliation

Note: The user logged in to the Admin Portal must have the **Grant** and **View** permission for the associated domain and the **Edit** permission for the system in order to configure the settings described in the following procedure.

1. Make sure the UNIX system where you are configuring password reconciliation is domain-joined.
2. In the Admin Portal, click **Resources> Systems** to display a list of systems.
3. Select the desired system and then click the **Advanced** page.
4. In the Administrative Account Settings area, next to **Local Administrative Account**, click **Provision**.

   The service creates a local administrative account with the reconciliation account name that you specified on the domain.

   Tip: You can also provision the local administrative account from the Advanced page by opening the Action menu and selecting **Provision Local Administrative Account**.

5. Under **Account Reconciliation Settings**, change the **Local Account Automatic Maintenance** setting to **Yes**.
6. Click **Save**.

Using UNIX Local Account Password Reconciliation Reports

Two built-in reports, “Account Password Reconciliation" and "Account Unlocks,” are provided to give you detailed information about UNIX local account password reconciliation-based accounts. You can view, copy, email, and export these reports.

Features of the reports include:

- Account Password Reconciliation - displays a list of account password reconciliations. Fields include: Date, Account, System, Type, FQDN, User, Mode, Admin Account, Admin Target, and Admin type.
- Account Unlocks - displays list of account unlocks. Fields include: Date, Account, System, Type, FQDN, User, Mode, Admin Account, Admin Target, and Admin type.

Changing UNIX System Settings

In addition to the common system settings you can change for any type of system, there are a few UNIX-specific system settings. For example, you can use System Settings to update or set the following types of information after adding a system:

- Select a domain for the system and enable domain operations.

  You can set a domain for a system and then enable domain operations to use the domain administrative account to enable zone role workflow. For configuration steps, see "Setting Domain Operations for a System" on page 556
- Change the session type or port number for remote connections.

  You can manually select secure shell or remote desktop and change the port number for remote sessions. If you don’t specify a session type and port, the secure shell client and port 22 are used by default.
- Select a system time zone.

  You can manually select the time zone you want to use for any system. If you don’t specify a time zone, the local time zone of the system is used by default.
- 'Use My Account' is configured on this system.

  You can select Use My Account to enable secure shell sessions that do not require a password. Users must have the view permission and an account on that system to log on. For details about how to configure a target system to Log on with the Use My Account feature, see "Authenticating with a Single-Use SSH Certificate" on page 85
- Change proxy account settings.

  If you configure SSH to prevent the root user account from logging on using secure shell connections, you can select the **Enable Proxy Account** option to set the proxy user name and password.
- Add or modify the optional description of the system.

Adding VMware VMkernel Systems

Overview

To manage VMware VMkernel accounts, you need to specify a valid local administrative account and password. See "Specifying a local administrative account" for more information. The account used must be in a role in the VMware VMkernel with the Host.Local.ManageUserGroups privilege.

For any account you add, you can also choose whether or not you want Privileged Access Service to manage the account password. If you select **Manage this credential**, Privileged Access Service automatically resets the password after the account and system are added and each time the account is checked in.

If you select **Manage this credential**, keep in mind that the Privileged Access Service can only manage passwords for privileged user accounts that have sufficient rights to configure and save settings. In addition, if there are any pending changes for other user accounts, those changes will be saved when Privileged Access Service updates a managed password.

For more information on managing VMware VMkernel systems, see the following topics:

- "Modifying system-specific details"
- "Password complexity rules"
- "Changing VMware VMkernel system settings"

Password Complexity Rules

All managed passwords generated by the Privileged Access Service consist of at least one upper case letter, one lower case letter, one number, one special character, and allow consecutive repeated characters regardless of the system type. In the **Admin Portal > Settings >Resources>Password Profiles**, the default password profile for VMware VMkernel systems restricts password length to a maximum of 39 characters. The following additional password rules apply:

- Minimum password length: 12 characters.
- Maximum password length: 39 characters.
- Supported special characters: !$%&()*+,-./:;<=>?[]^_{|}~

> **Note:** You should not use the following special characters in passwords that you define for VMware VMkernel user accounts: **' " `**

You should keep in mind that only Privileged Access Service will know the managed password being generated and stored. You should not select this option if you don't want Privileged Access Service to manage the password for the account.

Changing VMware VMkernel System Settings

In addition to the common system settings you can change for any type of system, there are a few VMware VMkernel system settings. For example, you can use System Settings to update the following types of information after adding a system:

- Change the session type or port number for remote connections

You can manually select secure shell or remote desktop and change the port number for remote sessions. If you don't specify a session type and port, the secure shell client and port 22 are used by default.

- Select a system time zone

You can manually select the time zone you want to use for any system. If you don't specify a time zone, the local time zone of the system is used by default.

- Account Management Settings

For password management, HTTPS port 443 is used. If you changed the port assignment used for password management, you need to manually set the Management Port field to match the setting of the VMware VMkernel system. Contact VMware VMkernel Support if you want to change the port setting.

Adding Windows Systems

For Windows systems, there are two types of accounts: **local accounts** and **domain accounts**. When you add users for a Windows system, the **user_name** you specify should always be a local user account. If you want to manage domain accounts for domain computers, you must first add the domain to the Privileged Access Service. For information about adding domains and domain accounts to the Privileged Access Service, see "Managing domains."

For more information about password management for local accounts on Windows systems, see the following topics:

- "Managing the password for local accounts"
- "Management port for password operations"
- "Configuring a proxy user for password operations"
- "Password complexity rules"
- "Changing Windows system settings"

Changing Windows System Settings

In addition to the common system settings you can change for any type of system, there are a few Windows-specific system settings. For example, you can use System Settings to update the following after adding a system:

- Select a domain for the system and enable domain operations.

  You can set a domain for a system and then enable domain operations to use the domain administrative account to enable zone role workflow. For configuration steps, see "Setting domain operations for a system."

- Change the session type or port number for remote connections.

  You can manually select secure shell or remote desktop and change the port number for remote sessions. If you don't specify a session type and port, the Remote Desktop Protocol (RDP) and port 3389 are used by default.

- Select a system time zone.

  You can manually select the time zone you want to use for any system. If you don't specify a time zone, the system time zone is UTC after you manually add the system. If the system is discovered, the system time zone is updated to the local time zone.

- Change proxy account settings.

  You can add a proxy user name and password to manage password validation and updates on a target system. If you don't specify a proxy user, the account credentials used to log on are used to manage passwords and validate accounts.

  If local account password reconciliation (LAPR) policies are enabled for domain-joined Windows systems, the proxy account settings are disabled and ignored if already configured.

- Select a protocol and port for password management.

  You can manually set the management mode to change the protocol and port used for password management on target systems. If you don't select a management mode, the default protocol and port that were identified when you added the system are used.

- Add or modify the optional description of the system.

  You can update the description for a target system at any time.

Configuring Proxy Users for Password Operations

You can specify a non-administrative **Proxy user name** and **Proxy password** to use when managing the password for the selected system. If you specify a proxy user account, you can also choose to have the password for that proxy account managed by the Privileged Access Service. If you don't specify a proxy user, the account credentials used to log on are used to manage passwords and validate accounts.

You should note that the proxy user account is only used for password management and account validation. It is not used for opening remote desktop sessions.

Note: If local account password reconciliation (LAPR) policies are enabled for domain-joined Windows systems, the proxy account settings are disabled and ignored if already configured.

Configuring Windows Local Account Reconciliation

You can reset out-of-sync managed local Windows account passwords stored in Privileged Access Service using the following methods:

- Delinea Client for Windows
- Local administrator account
- Domain administrator account

If the client isn't installed, you can use either a local or domain administrator account for account reconciliation.

You can use any of these methods to also unlock accounts. An account is locked after a specified number of unsuccessful login attempts.

This topic includes the following sections:

- "How account reconciliation works on Windows systems"
- "Configuring the Delinea Client for Windows for local Windows account reconciliation"
- "Configuring a local administrator for local Windows account reconciliation"
- "Configuring a domain administrator for local Windows account reconciliation"

Understanding Account Reconciliation on Windows

When a password change operation of an account fails, Delinea PAS retries the change operation periodically. If local account reconciliation (sometimes also called LAPR, or local account password reconciliation) is enabled on the system, then the Delinea PAS also reconciles the password as part of the password change operation. DelineaDelinea PAS initiates a password reset of local managed accounts if it detects an out-of-sync password during account login, account checkout, and rotate operations.

The service logs all events and you can view them in the **Resources> Systems > Activity** page. You can also build custom reports to view activity; for details, see "How to create a new report."

> **Note:** If you configure account reconciliation using the client and you also specify either a local administrator or domain administrator account, the service will try to use the client first to reset the account password. If for some reason the client is not available or encounters a connection issue, then the service will use either the local administrator or domain administrator account, whichever is configured. If both the local and domain administrator accounts are configured and the client account reconciliation already failed, the service uses the local administrator. If then the local administrator account fails to reconcile accounts, the service will stop there (it won't use the domain administrator to reconcile accounts).

For information on configuring password reconciliation, see the following instructions. If you're using the client and one of the administrator accounts, be sure to follow both sets of procedures.

Configuring the Delinea Client for Windows for Local Account Reconciliation

This section includes the procedure to enable password reconciliation to reset out-of-sync account passwords and unlock local account passwords stored in Privileged Access Service on Windows systems that have the Delinea Client for Windows installed and enrolled.

For Delinea Client for Windows installation information, see "Installing and using the Delinea Client for Windows"

> **Note:** If you configure the client to handle account reconciliation, any **Management Mode** settings in **Resources** > **Systems** > **Settings** do not apply.

To configure Windows account reconciliation with the Delinea Client for Windows:

1. In the Admin Portal, navigate to **Resources > Systems** and then select the system where you want to enable password reconciliation.
2. Click **Client Profile** to view the client details and make sure that the system has the client installed and enrolled.
3. Click **Advanced** and in the Account Reconciliation Settings area, select one or both of the following:
   - **Local Account Automatic Maintenance**: Select this option so that Delinea PAS can reset the local account passwords when needed.
   - **Local Account Manual Unlock**: Select this option so that Delinea PAS can unlock a locked account. An account is locked after a specified number of unsuccessful login attempts.

     Note: Although the **Verify Configuration** button is directly under the local account reconciliation settings, it doesn't affect the client settings; you use this button when you set the local or domain administrator account for local account reconciliation.
4. Click **Save**.

Configuring Local Administrators for Local Windows Account Reconciliation

For an additional layer of security, you can specify a local administrator account to manage the local Windows accounts. You can use any account that is in the local Administrators group.

Note: If using an account in the local Administrators account, you need to disable the following policy: *User Account Control: Run all administrators in Admin Approval Mode security policy setting* You don't need to do this for the built-in Administrator account. For more information, please see this "article."

Note: The Management Mode and Proxy settings configured for a system (located in **Resources** > **Systems** > **Settings**) *do* apply if local account password reconciliation is enabled *but only if the Management Mode is set to use SMB*. For management mode, the system defaults to SMB when password reconciliation is configured.

To configure a local administrator account for local Windows account reconciliation

1. In the Admin Portal, navigate to **Resources > Systems** and then select the system where you want to enable password reconciliation.
2. Click **Advanced** and in the Account Reconciliation Settings area, select one or both of the following:
   - **Local Account Automatic Maintenance**: Select this option so that Delinea PAS can reset the local account passwords when needed.
   - **Local Account Manual Unlock**: Select this option so that Delinea PAS can unlock a locked account. An account is locked after a specified number of unsuccessful login attempts.

     Note: Although the **Verify Configuration** button is directly under the local account reconciliation settings, it doesn't affect the client settings; you use this button when you set the local or domain administrator account for local account reconciliation.
3. In the Administrative Account Settings area, click **Set** next to **Local Administrative Account** and specify the desired account.
4. Click **Save**.

Configuring Domain Administrators for Local Windows Account Reconciliation

Using a domain administrator account, users with the proper permissions can reset account passwords and unlock local account passwords stored in Privileged Access Service. All password rotations are done using the domain administrator account too.

If a password change fails because the password is out of sync, the service generates an event, and performs a hard password reset on the local account password.

Note: The Management Mode and Proxy settings configured for a system (located in **Resources** > **Systems** > **Settings**) *do* apply if local account password reconciliation is enabled *but only if the Management Mode is set to use SMB*. For management mode, the system defaults to SMB when password reconciliation is configured.

For each Windows system that you want to configure for local account password reconciliation, you need to configure settings for both the domain and each individual system. The table below summarizes the changes for each. Below the table are the procedures to follow for each kind of setting.

Required Domain Settings	Required System Settings
Set an administrative account (see "Set domain administrative accounts](https://.....com/pas/current/resources-remote-clients/add-resources/adding-domains/domain-administrative-accounts/index.md).This account is used to unlock/reset passwords for domain accounts and local accounts on systems joined to this domain.Enable account management settings for domain accounts and Windows local accounts. See "Setting Domain-specific Advanced Options" on page 488.Make sure the corresponding settings are also enabled in **Systems > Advanced**.	Set a domain at the system level to indicate that the system is joined to a specific domain.To ensure that password operations succeed, also make sure the system is joined to the domain outside of the Privileged Access Service.Enable account management settings for the local account ([Setting system-specific advanced options." See [Additional system permissions"Verify the configuration using the **Verify Configuration** button.

The Privileged Access Service cannot reconcile domain administrative account passwords that may be locked or out of sync. If the domain administrative account encounters an issue, operations using the domain administrative account will fail and an error message is displayed when you browse to the ****Resources**** portion of the Admin Portal. To troubleshoot the issue, see "Troubleshooting domain administrative accounts."

Configuring Domains for Local Account Password Reconciliation

To configure the domain for local account password reconciliation:

> **Note:** The user logged in to the Admin Portal must have the **Edit** permission for the domain to configure Administrative Account Settings described in the following procedure.

1. In the Admin Portal, click **Resources>Domains** to display a list of domains.
2. Select the domain and then click the **Advanced** page.
3. If it isn't configured already, for the **Administrative Account**, click **Select** and enter the domain administrative account that will be used to manage Windows domain-joined systems (see "Set domain administrative accounts."

   The domain administrative account must be a member of the Administrators group on the system. By default, the AD Domain Admins group is a member of the local Administrators group.
4. Select the desired account reconciliation options:
   - **Domain Account Automatic Maintenance**: Select this option to manage the passwords for domain accounts. For more details, see see "Enable automatic account maintenance using the administrative account."
   - **Domain Account Manual Unlock**: Select this option to enable Privileged Access Service to unlock any locked domain accounts. For more details, see "Enable manual account unlock using the administrative account."
   - **Windows Local Account Automatic Maintenance**: Select this option to manage the passwords for local Windows accounts.

- **Windows Local Account Manual Unlock**: Select this option to enable Privileged Access Service to unlock any locked local Windows accounts.

5. Click **Save**.

Configuring System to Use the domain administrator account for Local Account Password Reconciliation

Note: The user logged in to the Admin Portal must have the **Grant** and **View** permission for the associated domain and the **Edit** permission for the system in order to configure the settings described in the following procedure.

To configure a system to use the domain administrator account for local account password reconciliation:

1. Make sure the Windows system where you are configuring password reconciliation is domain-joined.
2. In the Admin Portal, click **Resources> Systems** to display a list of systems.
3. Select the system and then click the **Advanced** page.
4. In **Domain Settings**, click **Select** and enter the domain administrative account that will be used to manage Windows domain-joined systems. (Also see "Setting system-specific advanced options"
5. In **Account Reconciliation**, enable one or both of the following settings to successfully manage the passwords for local system accounts:
   - Local Account Automatic Maintenance
   - Local Account Manual Unlock

   Make sure the corresponding settings for Local Accounts are enabled in the Admin Portal > Resources > Domains > Advanced page (described in the previous procedure).
6. In the Admin Portal, click **Resources> Systems > Permissions**, and select the **Unlock Account** permission for users you want to have the ability to manually unlock managed account passwords.

   This can be done globally or at the system level. See "Setting Global Account Permissions" on page 750 or [Setting system-specific permissions .")
7. Once the configuration is complete, select **Verify Configuration** in **Admin Portal** **>**Resources> Systems > Advanced** to check that local account password reconciliation is properly configured.

   Make sure the domain administrator account has the **View** permission in order to verify the configuration.

   If the settings are configured correctly, the message *Verification completed successfully.* displays. If the settings are not configured correctly, an error message displays. Update your configuration and try **Verify Configuration** again.

   Note: If you configure the system with both a local administrator and a domain administrator account, use the **Verify Configuration** button verifies the local administrator account. To verify the domain setting, you need to remove the local administrator.

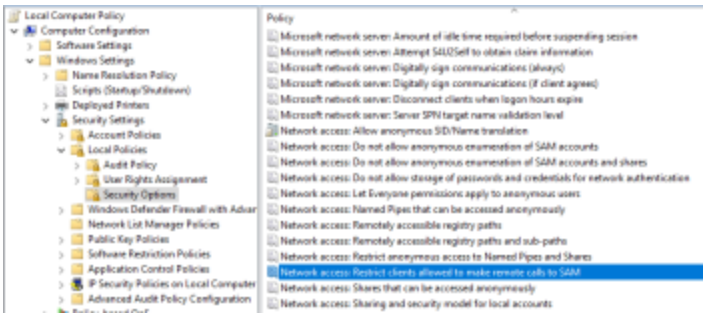
   Note: If you also configure password reconciliation on systems with Delinea Client for Windows, Delinea PAS will only use the domain administrative account to reconcile the out-of-sync password if it encounters a connection issue using the Delinea Client. See "Configuring the Delinea Client for Windows for local Windows account reconciliation" for configuration details.

Managing Local Accounts in SMB Mode

To manage local accounts in SMB management mode with a Windows 2016 server, add the local user accounts or the security group that contains the local users to the following policy setting:

Network access: Restrict clients allowed to make remote calls to SAM.

The above policy setting is located under **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options** > **Network access: Restrict clients allowed to make remote calls to SAM**.



Note: When managing local accounts in SMB mode and if the password complexity profile has a maximum password length of greater than or equal to 64 characters, then password rotation may fail.

Password Complexity Rules

For any account you add, you can also choose whether or not you want the Privileged Access Service. to manage the account password. If you select **Manage this credential**, the Privileged Access Service automatically resets the password after the account and system are added and each time the account is checked in.

All managed passwords generated by the Privileged Access Service consist of at least one upper case letter, one lower case letter, one number, and one special character regardless of the system type. For Windows systems, the following additional password rules apply:

- Minimum password length: 12 characters.
- Maximum password length: 32 characters.
- Supported special characters: !$%&()*+,-./:;<=>?[]^_{|}~

You should keep in mind that only the Privileged Access Service will know the managed password being generated and stored. You should not select this option if you don't want the Privileged Access Service to manage the password for the account.

Managing Ports for Password Operations

When you add Windows systems to the Privileged Access Service, the Add System wizard scans for available ports to determine the port to use for password-related operations. The management port is also used to change, update, or rotate the managed account password on the target system. Depending on the results of the scan, the protocol and port used to validate and manage password changes might be set to one of the following:

- Remote Procedure Call (RPC) protocol over TCP and port 135.
- Server Message Block (SMB) protocol and port 445.

- Windows Remote Management (WinRM) over HTTPS if port 5986 is open
- Windows Remote Management (WinRM) over HTTP if port 5985 is open.

If a suitable protocol and port cannot be found or the user account to be used for password management and validation does not have the appropriate permissions, the management mode for the system is automatically set to Disabled/Not Detected. Depending on the protocol you want to use for password management and validation, you might need to unblock a port or set up a proxy user and password with administrative privileges to run PowerShell commands, then retry automatic detection.

You can use System Settings after adding a system to manually set a management protocol and port or to select Auto-Detect to try to detect an appropriate port again if the first attempt failed.

If managing passwords using Remote Procedure Call (RPC) protocol over TCP and port 135, you must enable the default Netlogon Service Authz (RPC) firewall rule on the Windows system or create a firewall rule to open port 49152-65535 (TCP Dynamic) for inbound RPC endpoint connections.

For more information about port assignments and flow for password operations, see "Communication for password-related activity."

Mapping Local Groups

With local group mapping, you can map a cloud role to a local group on a Windows system. For example, you create a group in Privileged Access Service and call it "local admins" and map it the local group Administrators. Members of the cloud role “local admins” will be added to the local Windows group Administrators when they are logged into the system.

You must have the Delinea Client for Windows installed to use **Local Group Mapping**.

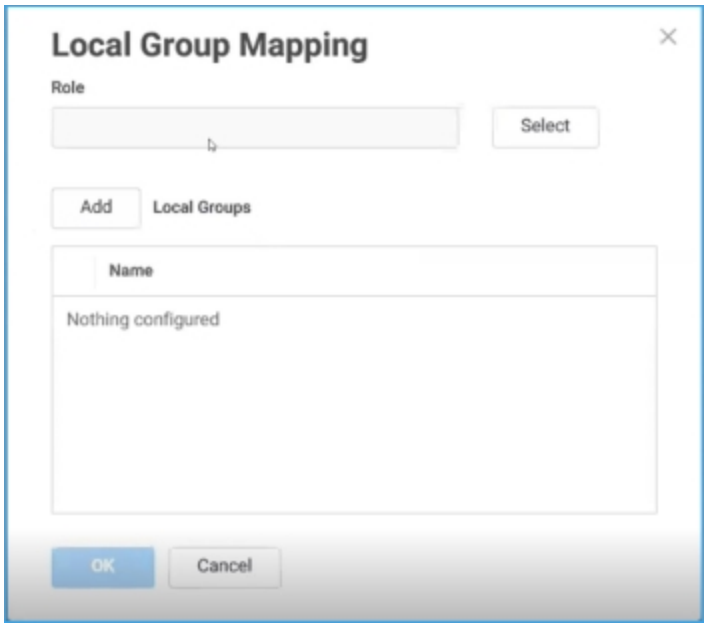
You can map local groups on Windows systems to users and roles in Delinea Directory or any federated directory service, such as LDAP, Okta, and so forth.

You can map Active Directory users to Windows local groups, as long as the system where you are mapping users to local groups is in a different Active Directory or not joined to Active Directory.

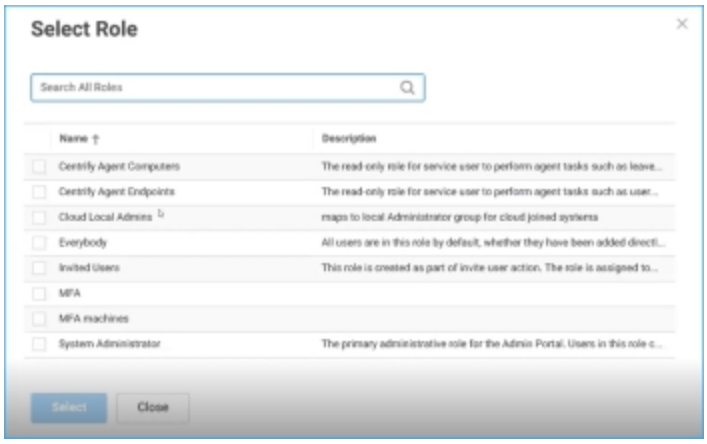
For an overview of local group mapping, see "About Windows local group mapping."

To map local Windows groups to Delinea PAS roles:

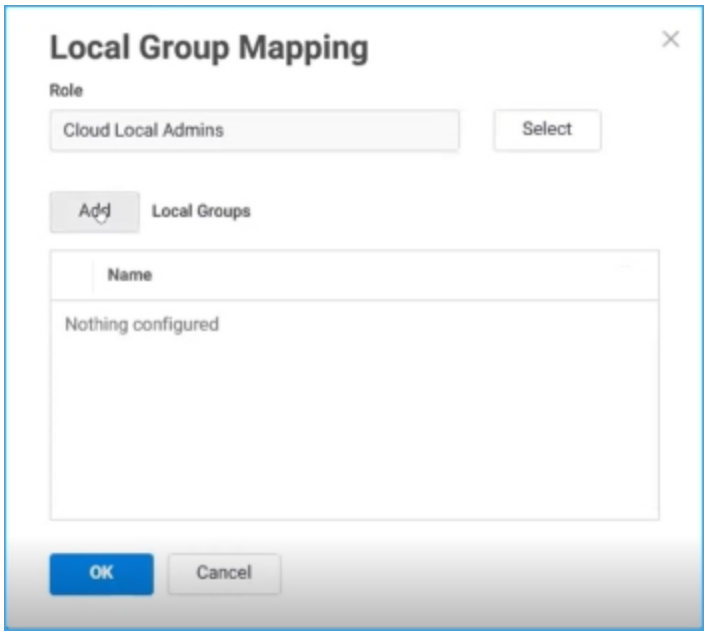
1. Navigate to **Resources** > **Systems**. Choose a system and click **Local Group Mapping** from the left-hand navigation.



2. Select the role you would like to add by clicking **Select** and choose the roles you would like to add:



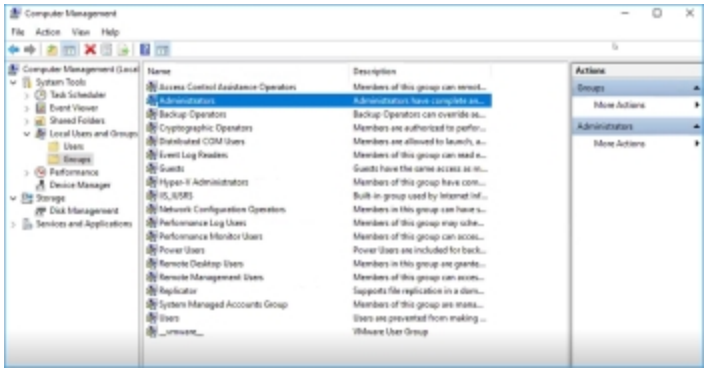
3. Then add the local groups and click **OK** and you will see the group mapping added.



Note: There is no verification on local group naming. If there is a typo in the group naming, the system will look for the group on the local system but may not match due to misspelling and the user will not be added. Additionally, if there is a space in the group name both words must be encased in double quote marks " ".

To verify the group membership, open the Computer Management utility and navigate to **Local Users and Groups**, and *either*:

- Select **Groups**, double-click on the group you're adding user to (Administrators in our example), or
- Select **Users**, double-click on the user and then switch to the **Member Of** tab.



Managing Passwords for Local Accounts

You can specify any valid local user account and password. In most cases, however, you would specify Administrator or an account with similar privileges for which you want to manage the password. If you select the **Manage this credential** option for an account, the Privileged Access Service handles all periodic password changes and validation for the account. You can configure a separate "proxy" account to perform these tasks on Windows systems, if needed.

For a failed password rotation attempt, which includes either a manual rotation, setting an automatic password rotation on check in, or 'enable period password rotation', PAS will start a background job that will try again in 5 minutes to try to rotate the password. If that attempt fails it will try again in 10 minutes. Continued failures result in a longer time period before trying again, and the maximum wait time to try again is 24 hours. PAS will try this a total of 40 times.

For other system types, the “proxy” account performs a similar function but is specifically used as a substitute for the root account.

For more information about password and system management for Windows systems, see the following topics:

- "Managing Ports for Password Operations" on page 551
- "Configuring Proxy Users for Password Operations" on page 546
- "Password Complexity Rules" on page 551
- "Changing Windows System Settings" on page 545
- "Managing Local Accounts in SMB Mode" on page 551

Connecting to Networks

With the Privileged Access Service, you can securely store local user name and password combinations (accounts). You can then use those accounts to connect interactively to servers, switches, and routers (systems). You can also choose who is authorized to use the accounts on which systems and who is authorized to view or copy the account password.

The systems you manage might include servers and network devices inside of your organization’s firewall, outside of the firewall, or a combination of the two. For example, you might have some users who can log on to specific systems inside of the firewall and others who can access specific systems located outside of the firewall.

In the most common scenario, you would add shared local accounts—such as root, patrol, or oracle—for the systems you add to the Privileged Access Service. You would also specify which users are allowed to use those shared accounts and what different users are allowed to do. For example, you can specify which users can connect using a given account without having to specify the password for the account.

Planning for Adding System Accounts

For supported infrastructure (for example: systems and databases), account names are often case sensitive. Ensure the account entered in Privileged Access Service matches the account in the infrastructure.

Selecting Connectors

By default, systems use any available connector without evaluating the network topology. If the communication with a current connector is interrupted, systems automatically select another available connector to continue operation. To give you more control over which connector different systems use, you can map specific system subnet patterns to specific connectors. Systems can then use the globally-defined network topology to identify the closest connector available and will use the next closest available connector if the communication with the closest connector is interrupted.

Global system subnet mapping gives you the best combination of performance and failover support in most cases. However, there are circumstances in which you might prefer to specifically designate the connectors individual systems should use. For example, if the “closest” connector in the network topology has bandwidth or latency

issues, you might want to designate one or more specific connectors for a system. You might also want to specify connectors for individual systems to control load balancing and failover support.

If you want to specify the connectors for an individual system, you can do so when viewing the details for the system. System-specific settings take precedence over any global connector subnet mapping you have configured.

In cases where site information isn't configured in Active Directory, you can

To specify the connectors to use for a system:

1. In the Admin Portal, click ***Resources***, then click **Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Click **Connectors**.
4. Select **Choose**, then select the specific connectors to use for the system from the list of available connectors.
5. Click **Save**.

Setting Domain Operations for a System

You can set a domain for a system and enable domain operations to use the domain administrative account to enable zone role workflow. To enable this option, make sure you have:

- Grant permission for the domain.
- Edit permission for the system.
- An administrative account for the domain (see "Set domain administrative accounts."

You need to configure the domain and enable operations before you can enable zone role workflow. For more information on zone role workflow, see Managing zone role assignment requests.

To enable domain operations for a system

1. In the **Admin Portal > Resources**, then click **Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Click **Advanced** and then click **Set** next to the Domain text box to select the relevant domain.
4. Start typing the domain name into the search box.

   The service lists the domains for which you have View permission.
5. Select the domain you want to use.
6. Click **Select** and then click **Save**.

   If the domain has a domain administrative account already configured, it is displayed in the Domain Administrative text box. If the domain selected for the system does not have a domain administrative account configured, see "Set domain administrative accounts."

Setting System-specific Policies

You can set policies for individual systems or set global policies to apply to all systems you add to the Privileged Access Service except where you have explicitly defined a system-specific policy. If you use a combination of global and system-specific policies, the system-specific policies take precedence over the global policies you set.

If you have the appropriate permissions to set global system policies, see "Setting global security options" for more information. If you are not using global policies, only want to set policies on individual systems, or want to override global policies on specific systems, you can set the following policies on a case-by-case basis:

- "Allow remote access from a public network"
- "Allow RDP client to sync local clipboard with remote session"
- "Checkout lifetime"
- "System login challenge rules and default profile"
- "Authentication if managing the service on-site"
- "Privilege Elevation challenge rules and default profile"
- "Enabling client automatic updates"

To set system-specific policies:

1. In the Admin Portal, click **Resources**, then click **Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Click **Policy**.
4. Select settings for any or all of the system policies.
5. Click **Save**.

For more information about how to set the system-specific policies, click the policy link or the information icon in the Admin Portal.

Allowing Remote Access from a Public Network

Select Yes if you want to allow remote connections from inside or outside of a defined corporate IP address range. If you select Yes, administrators can log on remotely to the selected system from computers or devices that are inside or outside of the corporate IP address range. If you select No, administrators will be denied access if they attempt to log on to the selected system from a connection outside of the corporate IP address range.

If you do not specify a corporate IP address range to define your internal network, all IP addresses are treated as external connections from outside of the firewall and remote access is denied by default.

Allowing RDP Clients to Sync Local Clipboards with Remote Sessions

Select Yes for the ability to copy and paste text or images while in a web based RDP session. When enabled, allows you to copy texts or images from a local machine and paste them to the remote session and vice versa. Applies to RDP native client and web clients as follows:

Browser	Text support	Image support
Chrome	Supported	Supported
Edge	Supported	Supported

Browser	Text support	Image support
Internet Explorer 11	Supported	Not supported
Safari	Not supported	Not supported
Firefox	Not supported	Not supported

Checkout Lifetime

Type the maximum number of minutes administrators are allowed to have a password checked out. After the number of minutes specified, the Privileged Access Service automatically checks the password back in. The minimum checkout lifetime is 15 minutes. If the policy is not defined, the default checkout lifetime is 60 minutes.

You can extend the checkout time for a password as long as you do so before the initial checkout period expires. For example, if the maximum checkout lifetime is 60 minutes and you extend the checkout time before the 60 minute period is over, the password expiration is reset to the 60 minute checkout lifetime. For more information about configuring the Checkout lifetime policy, see "Extending the password checkout time."

System Login Challenge Rules and Default Profiles

You can configure authentication rules and authentication profiles to protect remote login access for specific systems. Based on the rules you define, users attempting to log on to a system without knowing the stored account password or using specified credentials might be required to answer a security question, answer a phone call, or click a link in an email message to authentication their identity. The authentication rule defines the conditions for when a specific authentication profile should be used. The authentication profile defines the types of challenges presented and whether one-factor or two-factor authentication is required. You can also define a default authentication profile to use if the conditions you specify for the account login rules are not met.

If you don't create any authentication rules or authentication profiles for logging on without knowing the password for an account, users with the appropriate permission can log on using stored account passwords without being challenged to re-authenticate their identity. If you add authentication rules, a default authentication profile, or both, the policies are evaluated for all attempts to log on to the target system, whether using a stored account password or a specified user name and password.

Supported Authentication Challenges

You should note that only the authentication challenges that are available in a user profile can be presented. For example, you might select **Phone call** and **Email confirmation code** in the authentication profile, but these challenges are only valid if users have both a phone number and email address stored for their accounts.

If users only have a phone number and not an email address stored, they will receive a phone call to complete the authentication process rather than be prompted to select an authentication option. If users have both a phone number and an email address stored, they will be prompted to select which form of authentication to use.

Authenticating If Managing Services On-Site

If you have installed Privileged Access Service on your internal network or in a location where you are managing the service yourself, you can define authentication profiles that use most of the same challenges as when the Privileged Access Service is deployed as a cloud-based service. However, some challenges—such as the Email configuration

code and Text message confirmation code—require you to configure settings to support outgoing email and SMS-based text messaging.

You can configure the settings for a custom Simple Mail Transport Protocol (SMTP) mail server and a Twilio in the Admin Portal. To support the Mobile Authenticator as a challenge, you must have a properly registered mobile device. For details about post-installation configuration steps when you deploy Privileged Access Service as an on-site service, see the *Installation and Configuration Guide for On-Site Deployment*.

To add an authentication rule and profile for remote login access:

1. In the Admin Portal, click **Resources**, then click **Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Click **Policy**.
4. Under System Login Challenge Rules, click **Add Rule**.
5. Click **Add Rule** to define the conditions to evaluate to determine the authentication profile to use when users attempt to log on to a selected system using the stored account password.

   For example, click **Add Rule**, select a condition such as IP Address and inside of the corporate range, then click **Add**. You can add more than one condition to the rule. However, all conditions must be true for the rule to apply.
6. Select the authentication profile to use when all of the conditions you specify are true, then click **OK**.
   - You can select any existing authentication profile if an appropriate profile has been previously-defined in the Admin Portal for the Privileged Access Service.
   - You can select **Not Allowed** as the authentication profile if you want to prevent users from logging on using a stored account password when the conditions for this authentication rule are met. For example, you might want to select Not Allowed to prevent login access when the request comes from an IP address outside of the corporate IP range.
   - You can select **Add New Profile** if you want to create a new authentication profile to use when the selected conditions.

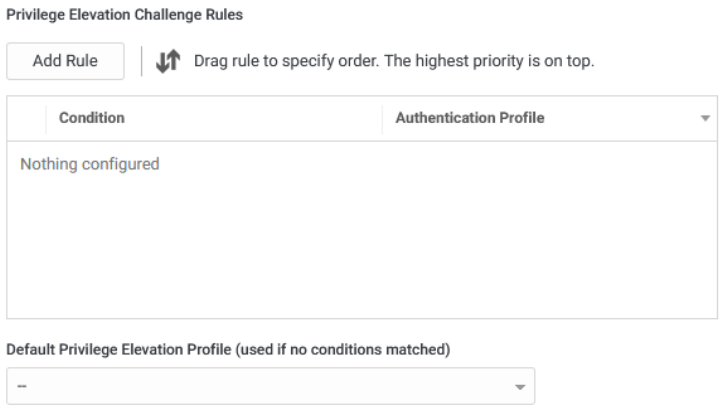
   If you are adding a new authentication profile, type a profile name, select the types of authentication challenges to present, set the challenge duration time to specify how long a previously-satisfied authentication challenge is valid, then click OK. For information about creating authentication profiles and specifying the types of authentication challenges for the authentication profiles you define, see "Creating authentication rules" and "Creating authentication profiles."

Privilege-Elevation Challenge Rules and Default Profiles

For systems and users that you have configured for privilege elevation, you can set up which conditions will result in which additional authentication credentials that users will have to enter when they try to run a privileged command or application. You also specify a default privilege elevation profile that applies if none of the specified conditions are met.

To configure privilege elevation challenge rules and default authentication profiles

1. Open the policy tab for the desired systems:
   - One system: In the **Systems** area, open the desired system, then click the **Policy** tab.
   - Some or all systems: In the **Policies** area, open or edit a policy set.
2. In the policy, navigate to **Resources** > **Systems**, and then the **Privilege Elevation Challenge Rules** section of the page.



3. In the **Privilege Elevation Challenge Rules** area, add rules that specify for a particular condition, apply a particular authentication profile.
4. For the **Default Privilege Elevation Profile**, specify which authentication profile applies if none of the conditions in the challenge rules are met.
5. Click **Save** to save your changes.

   The challenge rules and default authentication profile changes for privilege elevation take effect when the affected users next log try to run an application with privilege on an affected system.

Enabling Client Automatic Updates

Select **Yes** to specify that the service automatically updates the Client software on enrolled systems to the latest client version. After you select Yes, you can also specify a time of day to begin the automatic update.

Setting System-Specific Permissions

You can set system permissions for individual systems, sets of systems, or globally to serve as default permissions for all systems.

To set system-specific permissions:

1. In the Admin Portal, click ***Resources***, then click **Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Click **Permissions**.
4. Click Add to search for and select the users, groups, or roles to which you want to grant system-specific permissions, then click **Add**.
5. Select the appropriate permissions for each user, group, or role you have added, then click **Save**.

For more specific information about what different permissions allow users to do, see "Assigning permissions."

Setting System-specific Advanced Options

In the **Systems > Advanced** tab, you can select system-specific options for password security and maintenance and also view the zone status of a system.

The following sections provide information on configuring options in the Systems > Advanced tab:

- "Account Reconciliation"
- "Domain Settings"
- "Removing local accounts upon session termination - Windows only"
- "Allowing multiple password checkouts for this system"
- "Enabling periodic password rotation"
- "Enable password rotation after checkin"
- "Specifying the minimum password age (days)"
- "Specifying the password complexity profile"
- "Enabling periodic SSH key rotation"
- "Setting the minimum SSH Key Age (days)"
- "Specifying the SSH Key Generation Algorithm"
- "Enabling periodic password history cleanup"
- "Enabling periodic SSH key cleanup"
- "Enabling client automatic updates"

To configure system-specific advanced settings:

1. In the Admin Portal, click **Resources**, then click **Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Click **Advanced**.
4. Select settings for any or all of the password security and maintenance options.
5. Click **Save**.

For more information about how to set the system-specific options, click the information icon in the Admin Portal.

Account Reconciliation

Account reconciliation allows you to reset out-of-sync managed local Windows or Unix account passwords stored in Privileged Access Service. Account reconciliation for both Windows and Unix systems can be configured using either a local administrative account or through theCentrify Client for Windows or the Delinea Client for Linux.

To configure account reconciliation , you must enroll your system. If you do not have an enrolled agent, you will see a banner above the Account Reconciliation settings and must proceed to **Domain Settings** (below) to enable account reconciliation options. For information on enrolling your system, see "Enrolling and managing computers with Delinea Clients."

As part of the configuration process, you need to enable the following settings:

- Local Account Automatic Maintenance

  Allows users with the proper permissions to reset out-of-sync local account passwords stored in Privileged Access Service.

  > **Note:** For domain-joined Windows systems with account reconciliation configured using a domain administrative account, make sure the corresponding local account setting is also enabled in **Domains > Advanced > Administrative Account Settings > Enable Automatic Account Maintenance** (see "Enable automatic account maintenance using the administrative account."

- Local Account Manual Unlock (*Windows systems only*)

  Allows users with the proper permissions to unlock local account passwords stored in Privileged Access Service.

  For domain-joined Windows systems with account reconciliation configured using a domain administrative account, make sure the corresponding local account setting is also enabled in **Domains > Advanced > Administrative Account Settings > Enable Manual Account Unlock** (see "Enable manual account unlock using the administrative account."

To enable these operations, make sure you have:

- *Windows and Unix:* Edit permission for the system.
- *Windows via*Delinea Connector: Grant and View permission for the domain. Delinea
- *Windows viaDelinea Connector*: An administrative account for the domain with the View permission (see "Set domain administrative accounts."

(Windows systems using non-client based Account Reconciliation only) You can use the **Verify Configuration** button to check that local account password reconciliation is properly configured. Make sure the domain administrator account has the **View** permission in order to verify the configuration. If the settings are configured correctly, *Verification completed successfully.* is displayed. If the settings are not configured correctly, an error message is displayed. Update your configuration and try Verify Configuration again.

Configuration procedures differ for the various methods. For detailed information on configuring account password reconciliation for Windows and Unix systems, see:

- "Configuring Windows local account reconciliation"
- "Configuring UNIX local account reconciliation"

Local Administrator Account (required for non-client-based UNIX configurations)

Configuring the Local Administrator Account field is only required if you are configuring account reconciliation on UNIX systems that do not use the Delinea Client for Linux (in other words, this field applies to system configurations that use the Delinea Connector).

If you did not specify a local administrative account when you initially added the Unix system to the Privileged Access Service "Adding Systems with the Wizard" on page 519, you can set a local administrative account under

Account Reconciliation on the **Systems > Advanced** page. You need to configure a local administrator account before you can enable local account automatic maintenance. For more information, see [Configuring UNIX local account reconciliation."

You can specify an administrative account to perform account management tasks and reset out of sync managed local account passwords stored in Privileged Access Service. For additional information, see "Specifying a local administrative account."

Domain Settings

Under Domain Settings on the **Systems > Advanced** page, you can view the domain and the domain administrative account if it is configured. Setting these fields is required for Zone Role Workflow (also see "Enabling zone role workflow."

For Windows systems: The domain and domain administrative account fields are populated only if the system is domain joined and a domain administrative account is set for the domain; if it is not set these fields are empty. These fields are required for local account password reconciliation (LAPR) configured on Windows systems via the Delinea Connector and for Zone Role Workflow. If the system is already joined to a domain, the domain name is displayed in the text box. You must first add the appropriate domains to the Privileged Access Service in order to join the Windows system to a domain. For information on adding domains to the Privileged Access Service, see "Adding a domain."

To select a domain for a system:

1. In the **Admin Portal > Resources**, then click **Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Click **Advanced** and then click **Set** next to the Domain text box to select the relevant domain.
4. Start typing the domain name into the search box.

   The service lists the domains for which you have View permission.
5. Select the domain you want to use.
6. Click **Select** and then click **Save**.

   If the domain has a domain administrative account already configured, it is displayed in the Domain Administrative text box. If the domain selected for the system does not have a domain administrative account configured, see "Set domain administrative accounts."

Removing Local Accounts upon Session Termination (Windows only)

When a user logs in to a system by way of client-based login, the service creates a local Windows account to facilitate that login. You can choose to completely remove that local account when the user's session terminates. For more information about this account, see "Enabling client-based login."

Select **No** if you do not want to completely erase the local account. Keeping this account intact preserves any changes that the user made during their session, such as configurations or settings and also the user's home directory

Select **Yes** if you want to completely erase the local account that gets created when users log in to a system by way of client-based login (Agent Auth). Erasing this account involves removing the home directory and any personal configurations or settings.

Allowing Multiple Password Checkouts for Systems

Select **No** if only one administrator is allowed check out the password for a selected system at any given time. If you select **No**, the administrator must check the password in and have a new password generated before another administrator can access the system with the updated password.

Select **Yes** if you want to allow multiple users to have the account password checked out at the same time for a selected system. If you select **Yes**, multiple administrators can access the system without waiting for the password to be checked in.

Enabling Periodic Password Rotation

Select **Yes** if you want to rotate managed passwords automatically at the interval you specify. Select **No** if you want to prevent password rotation for the selected system.

If you select Yes, you should also specify the password rotation interval in days. Type the maximum number of days to allow between automated password changes for managed accounts. You can set this policy to comply with your organization's password expiration policies. For example, your organization might require passwords to be changed every 90 days. You can use this policy to automatically update managed passwords at a maximum of every 90 days. If the policy is not defined (--), passwords are rotated according to the setting in **Settings >** Resources**>Security Settings** tab.

Enabling Password Rotation after Check in

Select Yes to allow password rotation after it is checked in. Select No to not allow password rotation after it is checked in.

Specifying the minimum password age (days)

Specify the minimum number of days that a managed password must have been in use before it can be rotated.

Specifying the Password Complexity Profile

Select an existing password generation profile or add a new profile for the selected system. If you don’t select or add a profile, the default password generation profile for the system type is used. For more information about adding and editing password complexity profiles, see "Configuring password profiles."

Enabling Periodic SSH Key Rotation

Select **Yes** to allow periodic password rotation. Select **No** to not allow periodic password rotation. Select "**--**" to use the default setting from the Security Settings in the Settings tab.

Setting the Minimum SSH Key Age

Minimum amount of days old an SSH key must be before it is rotated.

Specifying the SSH Key Generation Algorithm

Specifies the algorithm to use when generating SSH keys during manual or automatic SSH key rotation.

Enabling Periodic Password History Cleanup

Select Yes to automatically delete retired passwords from the password history after a given number of days. Select No to prevent the Privileged Access Service from automatically deleting retired passwords from the password history at a set interval.

If you select yes, you can also specify the maximum number of days of password history to keep. For example, if you have a requirement to keep a record of passwords used for three years, you might set the cleanup interval to 1096 days to maintain the password history for that period of time. If you select the default setting, retired passwords are automatically deleted after 365 days. You cannot set a cleanup interval less than 90 days.

Enabling Periodic SSH Key Cleanup

Select **Yes** to allow periodic SSH key cleanup. Select **No** to not allow periodic SSH key cleanup. Select "**--**" to use the default setting from the Security Settings in the Settings tab.

Enabling Client Automatic Updates

Select **Yes** to specify that the service automatically updates the Delinea Client software on enrolled systems to the latest client version. After you select Yes, you can also specify a time of day to begin the automatic update. After the service updates the client, the system's Activity page displays information about the client version and the automatic update.

Specifying Local Admin Accounts

You can identify any account you add to the Privileged Access Service as the local administrative account for a specific system. However, some system types require you to specify a local administrative account if you want to manage any local account passwords. The account you designate as the local administrative account must have sufficient privileges to set and rotate passwords for other accounts. In addition, the local administrative account you specify for any system should be a dedicated account that is used exclusively by the Privileged Access Service.

You can have the password for the local administrative account managed by the Privileged Access Service to avoid password changes by other users who have administrative privileges. If you want to manage the password for the local administrative account, there are restrictions on the actions available. For example, you cannot select the **Login** action because that action could be used to compromise the login shell for the local administrative account. Similarly, because the local administrative account is used internally to manage passwords for other accounts, you cannot select the **Checkout**, **Rotate Password**, or **Delete** actions when you select an account currently designated as the local administrative account.

If you need to set or change the local administrative account after adding a system, you must have the **Edit** permission on the system and the **Grant** permission on the account. You have these permissions by default if you are the owner who adds the system and account to the Privileged Access Service.

Only the systems that require a local administrative account support this option.

System type	Administrative account
UNIX	You must specify a valid local administrative account to manage password operations for other accounts. Domain Administrative accounts for Unix are also supported, see "Set domain administrative accounts."
Windows	You cannot add a local administrative account for Windows systems. Domain Administrative accounts for Windows are supported, see "Set domain administrative accounts."
Cisco AsyncOS	You must specify a valid local administrative account to manage password operations for other accounts.
Cisco IOS	You cannot add a local administrative account for Cisco IOS systems.
Cisco NX-OS	You cannot add a local administrative account for Cisco NX-OS systems.
Juniper Junos OS	You cannot add a local administrative account for Juniper Junos OS systems.
HP NonStop OS	You cannot add a local administrative account for HP NonStop OS systems.
IBM i	You cannot add a local administrative account for IBM i systems.
Generic SSH	You cannot add a local administrative account for Generic SSH systems.
Check Point Gaia	You must specify a local administrative account to manage the password for expert mode operations. The administrative account is not required to manage the password for other accounts.
Palo Alto Networks PAN-OS	You must specify a valid local administrative account to manage password operations for other accounts.
F5 Networks BIG-IP	You must specify a valid local administrative account that is a member of the Administrator role to manage password operations for other accounts.
VMware VMkernel	You must specify a valid local administrative account to manage password operations for other accounts.

For more information about system settings, see the system-specific settings.

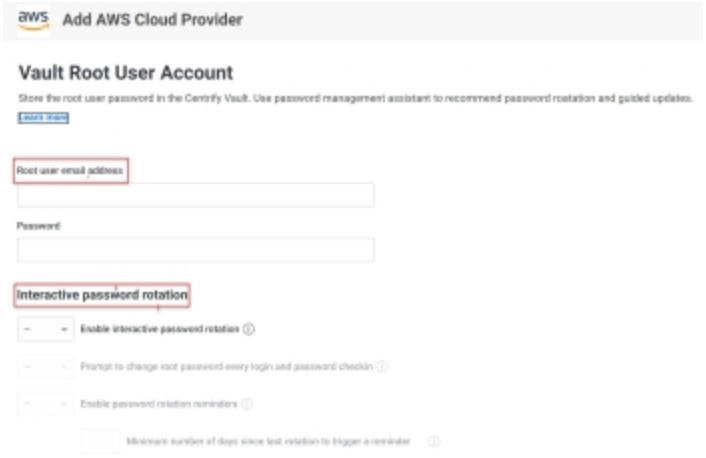
Managing a Cloud Provider Account

You can add and configure the Amazon Web Services cloud provider in the Privileged Access Service system by performing the following steps.

To add a cloud provider

1. In the Admin Portal, click **Resources** > **Cloud Providers**. Click **Add Cloud Provider**: add a **Name** and **Account ID**. Click **Next**.
2. You can choose to vault your root user account or click **Next** . Note the Delinea Browser Extension is required to perform root account login and password rotation capabilities. Vault the root user password by entering the **Root user email address** and **Password**. After specifying the root account credentials, you can optionally select to enable interactive password management, which provides automated guidance for updating and managing the root account password. Under **Interactive password rotation** , set values for **Enable interactive password rotation**. By selecting **Yes**, you can further set the following:

- **Prompt to change root password every login and password checkin**: Displays a prompt with an option to interactively rotate the root account password after every root account login attempt or password check-in.
- **Enable password rotation reminders**: Displays a banner message with an option to interactively rotate the root account password after the specified minimum number of days since last rotation has expired. Enabling this also allows you to set the minimum number of days since last rotation to trigger a reminder.



Once you have made all the password rotation settings, click **Next**.

1. Next, assign permissions to the root user account. Click **Add** to add a user, group, or role through the wizard. Click the checkboxes of permissions you wish to assign the user and lick **Next**.
2. And finally, optionally configure MFA challenge rules for root account login and password checkout. Click **Add Rule** to configure challenge conditions and set authentication profiles. Click **Add Filter** to add a filter. For more information on authentication rules, see "Creating Authentication Rules" on page 281
3. Click **Done**.

Once you have added a cloud provider you can perform the following actions on an individual cloud provider: **Add to Set**, **Delete**, and if you vaulted your root account you can **Login** to that cloud provider. Additionally, you can:

- vault IAM users,
- manage root accounts,
- add IAM users,
- assign permissions,
- manage activity,
- assign policy,
- view policy summary, and
- add/modify sets of cloud providers.

To learn more about cloud provider capabilities select from the following topics:

Vaulting IAM users:

Here, you add and vault IAM users. For more information on vaulting IAM users, see "Vaulting IAM User-Access-Key Secrets" on page 580

Managing your cloud provider root account:

For Delinea PAS root accounts, you can vault a password. The vault root user account allows you to store the root user password in the Delinea vault. You can then retrieve and check in that password whenever you like. For more information on root user accounts, see "Vaulting a Cloud-Provider Root-User Account" on page 572

Adding an IAM user to your cloud provider account:

Allows you to add and retrieve access keys for your cloud provider account. Additionally, you can delete access keys for your account. For information on how to add an IAM user to your cloud provider account, see "Adding and managing IAM users for a cloud provider account."

Managing permissions on your cloud provider account:

Allows you to add permissions to your cloud provider account. For more information on permissions, see "Assigning Permissions" on page 743

Viewing cloud provider activity:

Allows you to view cloud provider activity including the account email address that was added along with the time it was added.

Assigning policy on your cloud provider account:

Allows you to add policy to your cloud provider account. For more information on policy, see "Creating Authentication Rules" on page 281

Viewing cloud provider policy summary:

For users and resources, the summary shows the summation of all policies applied and the name of the policy set applying the policy. By default, the summary for an individual resource is for the logged-in user viewing the summary as shown in the selected user field at the top of the screen.

Adding and modifying sets of cloud providers:

You can add a cloud provider to a set. Additionally, there are two account sets for cloud providers:

- AWS IAM Accounts - this report lists the AWS IAM accounts that have been added to the cloud provider instance.
- AWS Root Accounts - this report lists the root accounts that have been vaulted with Delinea PAS.

Viewing Cloud Provider Reports

Navigate to the Admin Portal > **Reports** > **Builtin Reports** > **Resources** where you can view the following report for cloud providers: **Accounts by Cloud Provider** - where you can view all the accounts by cloud provider including account Name, Account, Credential Type, and Is Root Account.

Adding IAM User Accounts

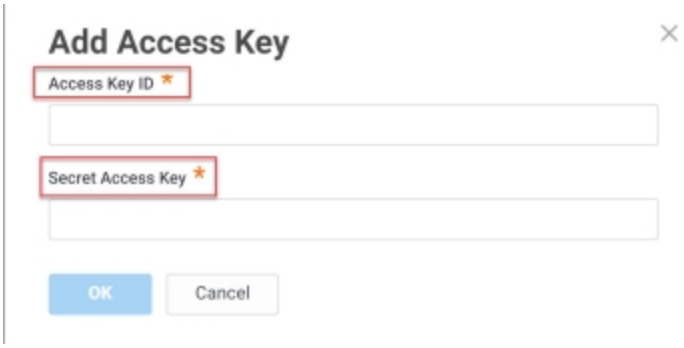
IAM accounts allow you to retrieve vaulted access key secrets. IAM accounts have up to two related access keys with:

- Each access key containing an ID and a secret. The secret is vaulted by Delinea PAS.
- Each vaulted secret has permissions and policies set for it.

Once you add an IAM user, you can view or edit: permissions, settings, access keys, policy, workflow, activity, and policy summary for the IAM account.

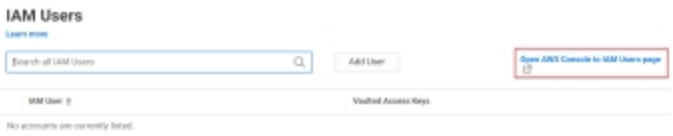
To add an IAM account

1. In the Admin Portal, navigate to **Resources** > **CloudProviders** and you will see a list of cloud providers. Select the cloud provider you wish to modify.
2. Click the **IAM Users** tab and click **Add**.
3. Enter a **UserName**. The user name must be actual IAM username.
4. For **AccessKey**, click **Add**.



Enter the **Access Key ID** and **Secret Access Key** from your provider and click **OK**.

Note: You can easily navigate to the AWS IAM users page by clicking **Open AWS Console to IAM Users page**in the top-right corner of the page as seen in the image below.



Once added, you can drill deeper into an IAM user account by clicking the account. Here, you can set the following for the IAM account:

Managing permissions on your IAM account:

Allows you to add permissions to your IAM account (Grant, View, Edit, Delete, Retrieve, Starts, Expires, and Inherited From). The permission **Retrieve** allows you to retrieve the secret for an Access Key for the IAM user (more information on retrieving an access key below). For more information on permissions, see "Assigning Permissions" on page 743.

Managing settings on your IAM account:

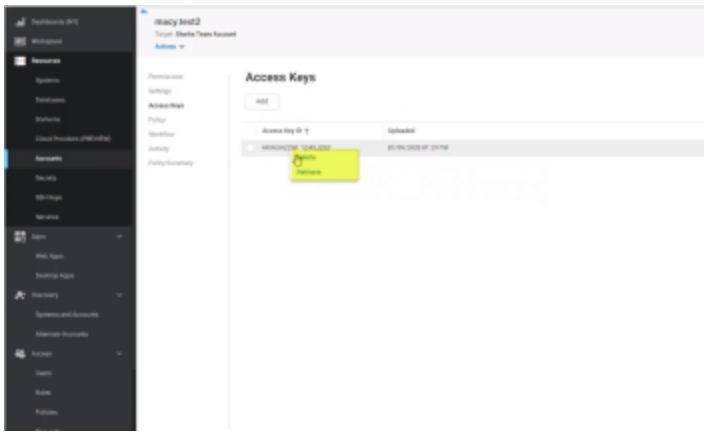
Here you can view or modify account settings.

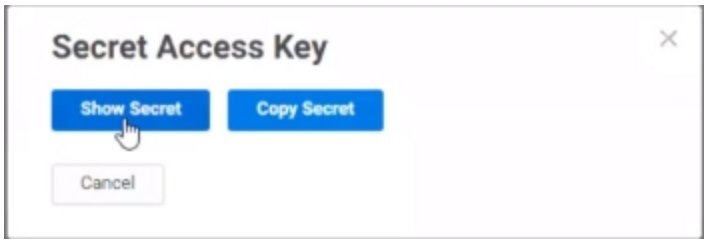
Manage access keys for your IAM account]:

Allows you to add and retrieve access keys for your IAM account as detailed below:

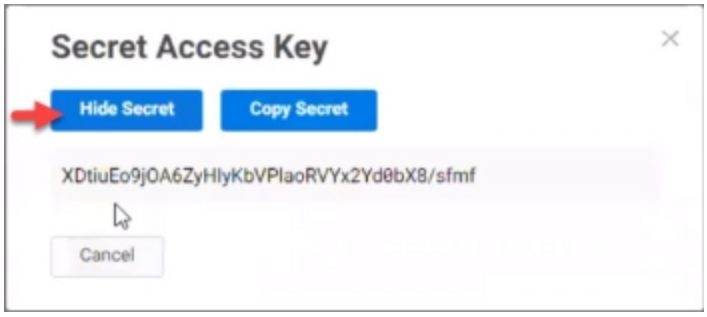
Retrieving Access Keys

1. In the Admin Portal, navigate to **Resources** > **CloudProviders** and you will see a list of cloud providers. Select the cloud provider you wish to modify.
2. Click **IAM Users** and select the user you wish to retrieve an access key for.
3. From the left-hand navigation, select **Access Keys**, right-click on the access key ID and click **Retrieve**:

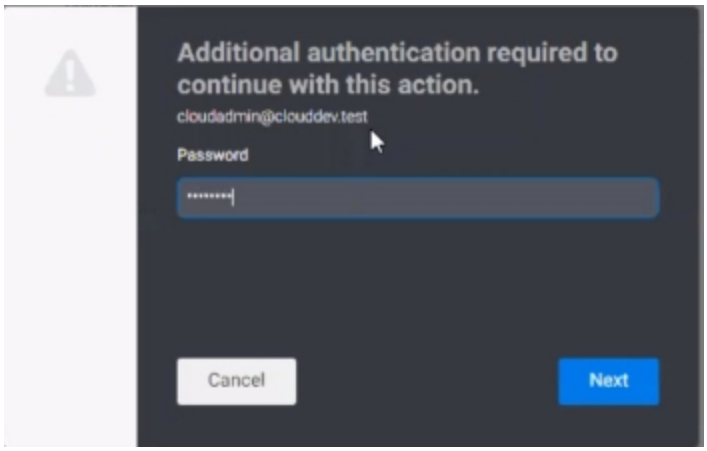




Note: As an added measure of security, after a short time, **Show Secret** reverts to hide the secret and will only show again when you click **ShowSecret**.



4. Next, you will get an MFA challenge, enter the password and click **Next**:



5. Finally, the access key is displayed with the ability to hide and copy the secret:

Deleting Access Keys

1. In the Admin Portal, navigate to **Resources** > **CloudProviders** and you will see a list of cloud providers. Select the cloud provider you wish to modify.
2. Click **IAM Users** and select the user you wish to retrieve an access key for.
3. Select **Access Keys**, right-click on the access key ID and click **Delete**.

Managing Policy on your IAM Account:

Allows you to add policy to your IAM account. For more information on managing policy, see "Creating Authentication Rules" on page 281.

Managing workflow for your IAM account:

Use to enable workflow for the IAM account. For more information on workflow, see "Enabling Request and Approval Workflow" on page 475.

Managing activity for your IAM account:

Use to view IAM account activity. The following are activity updates specific to IAM accounts:

- Retrieving an access key.
- Adding an access key.
- Updating the IAM account.

Viewing policy summary for your IAM account:

Use this to view the summation of all policies applied and the name of the policy set applying the policy.

Vaulting a Cloud-Provider Root-User Account

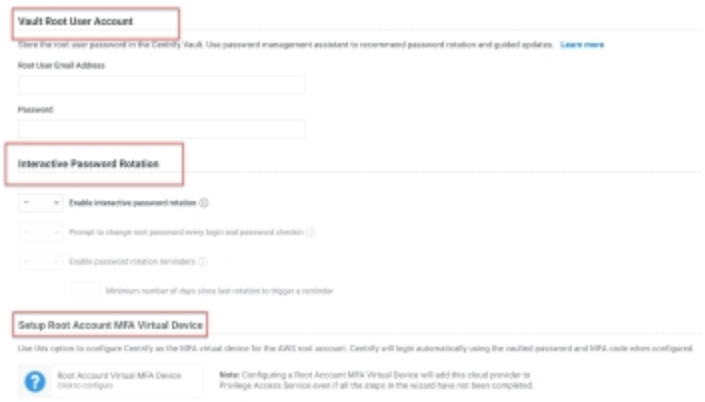
In Delinea PAS, root accounts allow you to vault a password. Vaulting the cloud provider root account in Delinea PAS allows you to securely store the root account credentials and manage access. Additionally, you can configure Delinea as the MFA device for the AWS account.

To vault or edit a cloud provider root user account

1. In the Admin Portal, navigate to **Resources** > **CloudProviders**. Select an existing cloud provider.

   Note: You can also vault a cloud provider root user account when you are adding a new cloud provider. For information on adding a new cloud provider, see "Managing a Cloud Provider Account" on page 567

2. Click **Root Account** and click **Vault Root User Account**. Enter **Root User Email Address** and **Password.**
3. Under **Interactive Password Rotation**, choose **Yes** to **Enable interactive password rotation** on demand rotation of your root account password from Delinea PAS.



4. For **Prompt to change root password every login and password checkin**, choose **Yes**. If this is enabled, you will be prompted to interactively rotate the password each time you login and checkin. When you click **Yes** to rotate password, you are taken back to the update password screen in the AWS console and the root account password is automatically rotated, concluding at the AWS account information page:

5. Select **Yes** for **Enable password rotation reminders** to set a minimum number of days since last rotation to trigger a reminder. The reminder is a banner that displays in the cloud provider user interface.
6. And finally, click the **Root Account Virtual MFA Device** button to configure Delinea as the MFA virtual device for the AWS root account.

Once you have vaulted a cloud provider root user account, you can right-click the account and perform the following actions:

Login:

If you have the Login permission set for the cloud provider, you can log into the cloud provider root account.

Checkout:

If you have the Checkout permission, you can check out the password for a stored account to use it for access to a system. When you check out a password, you choose whether to display or copy it to the clipboard for use.

Note: **Show Password** is only active for 15 seconds. PAS will hide the password after 15 seconds as a security measure.

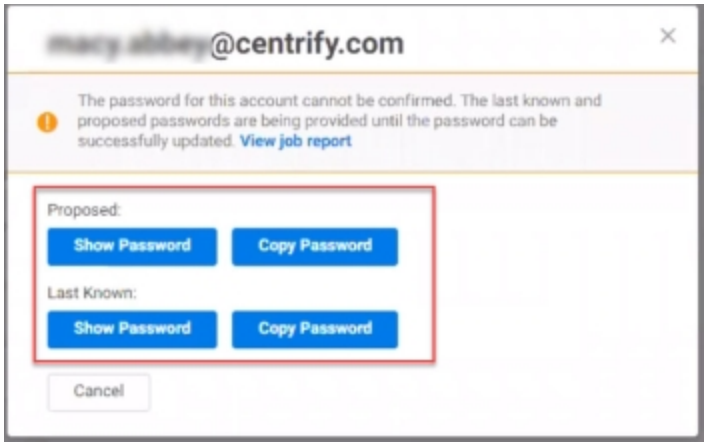
Update Password:

This allows you to update the root user's password.

Rotate Password:

This allows you to rotate the root user password. Unlike account password rotations, the root user account rotation is done on the user interface. If you lose connection with your browser after you have clicked **Rotate Password,** the password is not lost. You can retrieve it by doing the following:

1. Right-click and select **Checkout**, you will receive an error message, click **Close** on the error message. PAS is in an "uncertain password state."
2. Go back, right-click and select **Checkout** again and click **Show Password.** You will then see a screen asking which password you want to checkout, the proposed or last known password:



3. Copy the password. Go back to the account, right-click and choose **Update Password**.
4. The account is no longer in an uncertain state. Go back, right-click the account and **Checkin**.

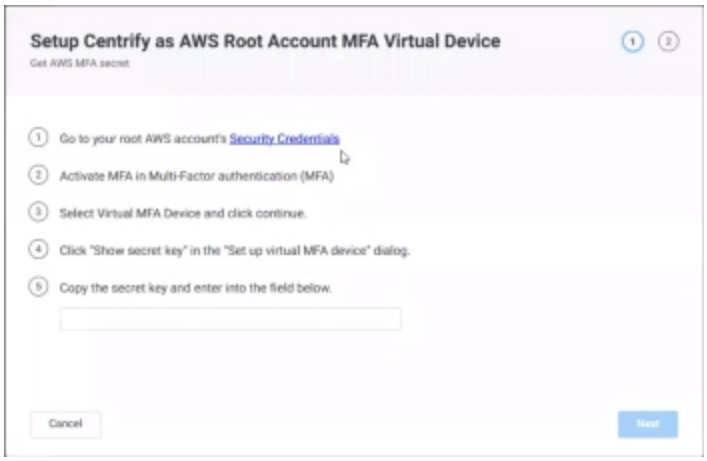
Add to Set:

This allows you to add this root account to a set of accounts.

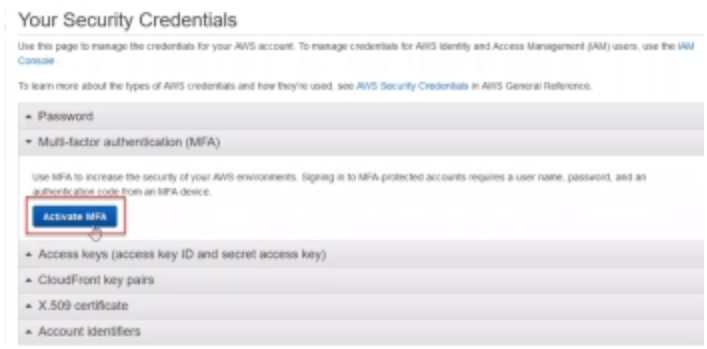
Set MFA Token:

This enables Delinea as the MFA device. When you choose this option:

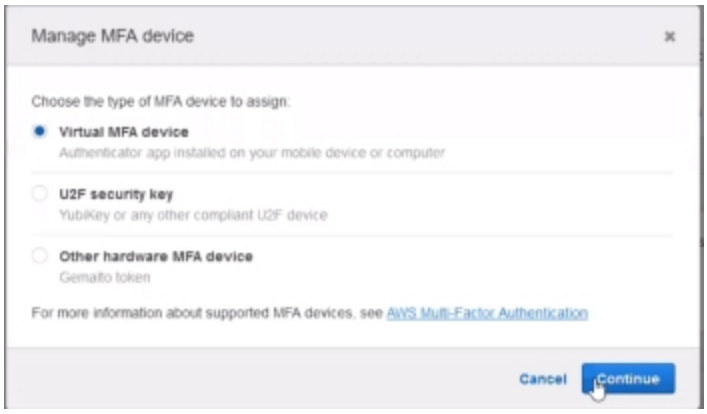
1. The **Delinea as AWS Root Account MFA Virtual Device** wizard:



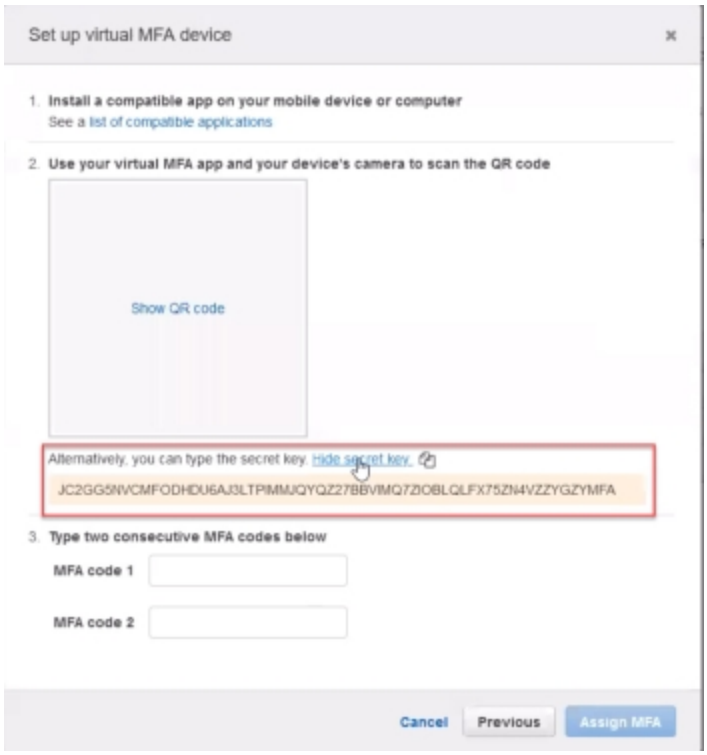
2. Clicking **Security Credentials** takes you to the root cloud provider's account page. There, you **Activate MFA**,



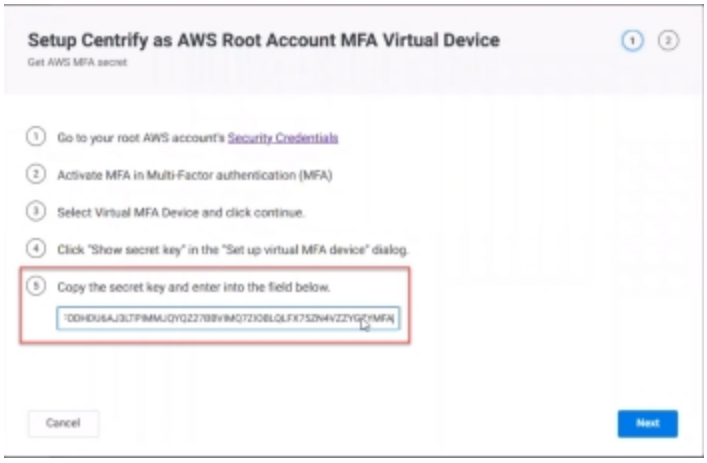
choose MFA type and click **Continue**.



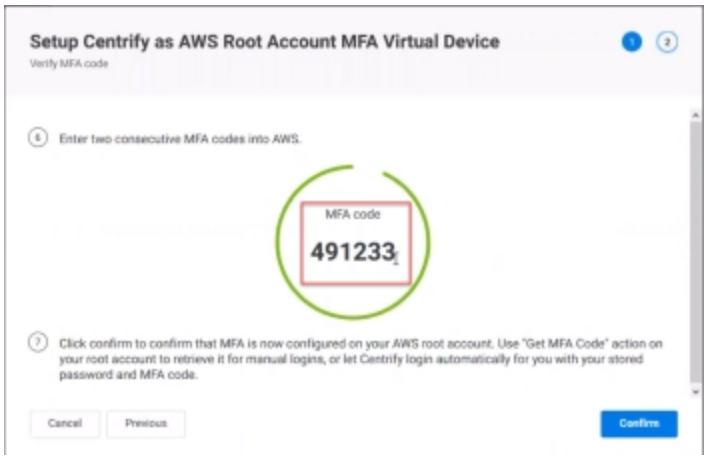
3. Set up the virtual MFA device by entering two consecutive MFA codes that you get by copying the secret key from the cloud provider:



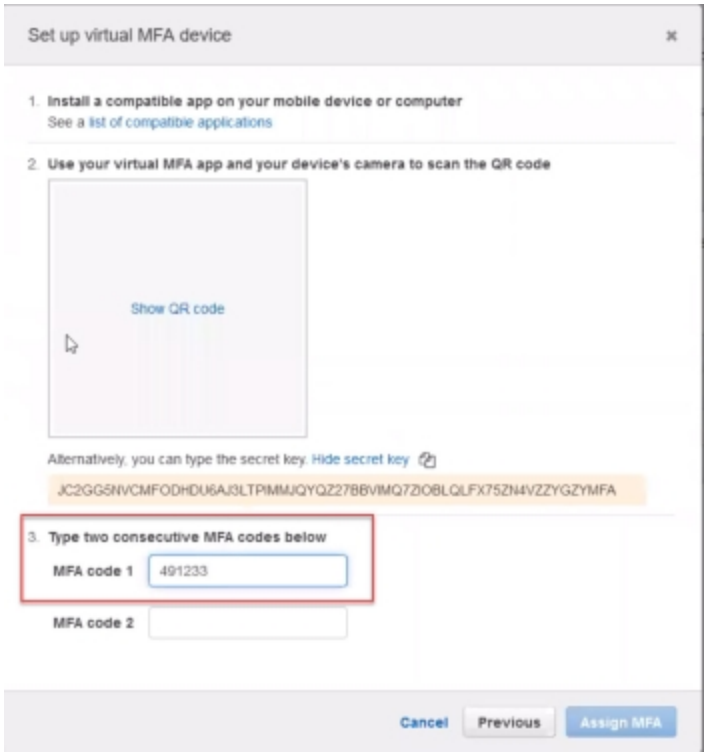
and pasting it into the Delinea wizard and click **Next**:



copy the code generated by Delinea:



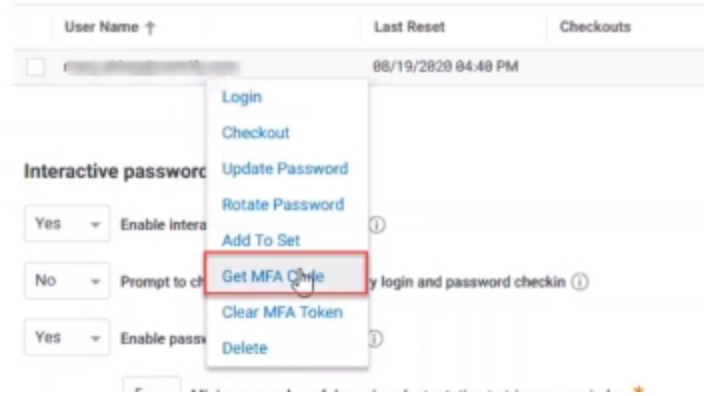
and paste it back into the cloud provider set up page:



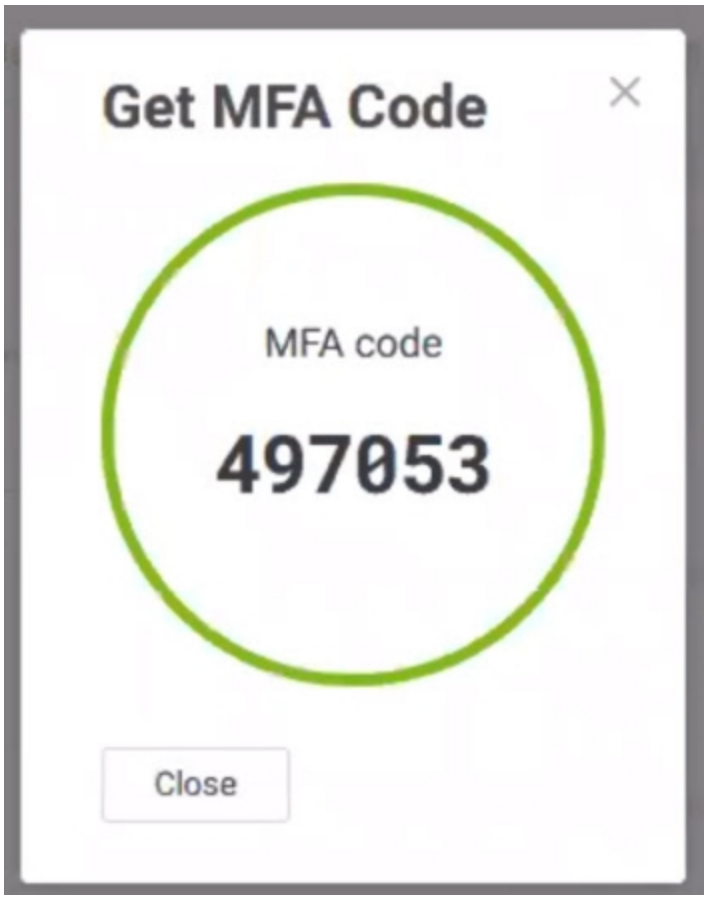
Once again, AWS requires two consecutive MFA codes be generated and pasted back into their set up page. As such, do this whole step once more to enter two codes and click **Assign MFA** when complete. You will see a success screen indicating it was a success and that Delinea is now the MFA virtual device for this account.

4. Go back into Delinea and click **Confirm**.

Now, the PAS vault has the MFA secret and it can issue MFA codes. To do this, right-click on the account and click **Get MFA Code** :



and this account generates MFA codes to use to login manually:



Delete:

Use to delete the root user account.

Once vaulted, you can drill deeper into a root account by clicking the account. Here, you can view or set the following for the root account:

Managing permissions on your root user account:

Allows you to add permissions to your root user account. These permissions are specific to the AWS account. For more information on permissions, see "Assigning Permissions" on page 743

Managing settings on your root user account:

Use to view account settings for the root user account.

Viewing password history on your root user account:

Use to view retired passwords for the root user account.

Managing policy on your root user account:

Allows you to add policy to the root user account. For more information on managing policy, see "Creating Authentication Rules" on page 281

Enabling workflow on your root user account:

Use to enable workflow for the root user account. For more information on workflow, see "Enabling Request and Approval Workflow" on page 475

Viewing activity on your root user account:

Use to view root user account activity. The following are activities updates specific to the root user accounts:

- Update.
- Permission granted.
- Viewing the password.
- Checking out the password.
- Login.
- Password rotation.

Viewing policy summary for your root user account:

Use to view root user account policy summary.

Vaulting IAM User-Access-Key Secrets

When you create an IAM user access key, the Secret Access Key is lost once the Create Access Key dialog is closed. Delinea PAS allows you to vault up to two IAM user Access Key Secrets so you never misplace them. Additionally, Delinea PAS extends policy to those access key secrets.

To vault or update a vaulted IAM user Access Key Secret

1. In the Admin Portal, navigate to **Resources** > **CloudProviders**. Select an existing cloud provider.
2. Navigate to **IAM Users** and select an existing IAM user account.
3. Navigate to **Settings**. Here, you enter the AWS Account ID for **Account ID**. Add a name and description if you wish and click **Save**.

Note: To quickly access this IAM user account in the AWS console, select **Open AWS Management Console page** in the top-right corner of the page as seen in the image above.

Configuring Secret Server

The Delinea PAS can connect to your remote and on-premise Secret Server(s) so you can use Secret Server as the authoritative source for storing and managing credentials.

Connecting Delinea PAS to Secret Server enables you to:

- See systems and accounts from one or more Secret Server vaults.
- Periodically sync systems and accounts from Secret Server. The sync may also be performed on-demand.

  Note: Passwords and SSH keys are not synced. They are retrieved from Secret Server when needed for login / checkout.

- Map to Secret Server sites using System Resource Mappings. These optional mappings give the Delinea PAS the information needed to choose an appropriate connector, when establishing a connection to a target system.
- Reach Secret Server directly for a SAAS Secret Server or via a connector for an on-premise Secret Server.

Syncing with Enabled Features

The following features are not currently supported for sync:

- Secret **Require Comment**
- Secret **Double Lock**
- Secret **Require Approval**

The features above sync as follows:

- If a Secret has the feature setting enabled, it will not be synced.
- If the feature is enabled after a Secret was synced, the Secret will be deleted from the Vault during the next sync operation.

Other Secret security settings can be enabled or disabled, and do not impact the sync operation. For example:

- Require Checkout
- Session Recording
- Hide Launcher Password

Syncing Secret Server Events

- Secret Audit events are generated when a secret is synced or accessed from the Vault.

  For example, when a Secret is synced, the Secret's audit will show an event for Secret View and / or password display operations.
- You can set up event subscriptions from Secret Server to get email notifications for the events generated when a secret is synced from the Vault. For example, the user can setup an event subscription for the Password Displayed event on the Secret, then receive an email notification for the sync operation.

Handling Passwords During Sync

When a Secret is synced to the Vault, the password is not saved on the Account created. The password is accessed by the Vault each time it needs to be used. This enables the Secret Server Password Expiration to continue working.

Note: If the secret synced to Vault expires, then password is changed in the Secret (i.e. by a Remote Password Change action), the next time that Vault needs to use the password, it will access the new password that was updated on the Secret.

To connect Delinea PAS to Secret Server:

Note: See the Secret Server Best Practices for information about configuring Secret Server for integration with the Delinea PAS.

1. Set Secret Server role permissions by enabling Delinea PAS administrators to add a vault.
2. Add a Delinea PAS vault and register the Secret Server.
3. For on-premise Secret Servers, deploy connector(s) that can reach the Secret Server.
4. Depending on network topology, configure the necessary Secret Server Resource Connector Mappings.

Adding Vaults

You can create a vault, which will enable you to connect to Secret Server.

To add a vault:

1. From the Admin Portal, navigate to **Resources** > **Vaults** > **Add Vault**.
2. Fill in the following fields:
   - **Name** - Your vault name
   - **Description** - Optional. Description for your vault.
   - **Vault Type** - The type of vault. For example, Secret Server.
   - **Vault Location** - Specify if your vault is a cloud instance or on-premises.
   - **URL** - The connection URL. Ensure you include the `http`or `https`prefix.
   - **User Name** - The user name to log into the specified URL.
   - **Password** - The password to log into the specified URL.
   - **Enable Sync Interval** - Indicates if you want to sync at regular intervals. The default value is off.
   - **Sync Interval** - Enter this value if the Enable Sync Interval switch is on. Specify the value in hours.

     Note: Synchronization can handle around 5,000 secrets within about 3 hours. Your synchronization time should be *longer* than the total time it takes for a single synchronization to complete.
3. Click **Next** to go to the Template Mapping page.

   Note: If this is an on-premises vault, the template section will be disabled. You will need to add the vault and configure your settings first, prior to selecting templates.

   a. Template mapping:

      Choose the system and account templates you want synchronize.

      We suggest leveraging a legacy Report in Secret Server to see how Secrets are spread across different templates within your environment. This will help indicate which templates you should map for your integration.

      The available template categories are:

- Windows Systems
- Unix Systems (Password Credentials)
- Unix Systems (SSH Key Credentials)
- Active Directories

b. **Add sets:** (Optional) Add sets using the field under **Add to Sets**.

4. Click **Done**.

Deploying Connectors

Delinea connectors can be used to reach out to on-premise Secret Server instances. On-premise servers require connectors because the Delinea PAS can't directly resolve / reach the address for on-premise servers.

You can specify the connection type for each vault. Below are two examples:

- A cloud Privileged Access Service tenant which connects to a cloud Secret Server tenant.
- A cloud Privileged Access Service tenant which connects to an on-premise Secret Server tenant via a connector.

Setting Secret Server Role Permissions

Ensure only Delinea PAS administrators you want to administer the integration have appropriate permissions to add vaults.

Note: We strongly suggest you create a new role for this type of access.

To create a new role for Secret Server:

1. From the Admin Portal navigate to **Access** > **Roles**.
2. Click **Add Role**.
3. On the **Description** tab, name the Role and add an optional **Description**.
4. On the **Members** tab, use the **Add** button to add the appropriate Delinea PAS administrators.

   Note: We recommend leveraging groups where possible.
5. On the **Administrative Rights** tab, click **Add**.
6. Select the **Add Vaults** option, then click **Add**.
7. Click **Save**.

Configuring Template Mappings

System Resource Mappings include a resource mapping for Secret Server sites. These mappings are optional.

Mappings provide the Delinea PAS information needed to choose an appropriate connector, when establishing a connection to a target system. The Resource Mappings will:

- Get the information from Secret Server site(s).
- Display the information so you can use it to map to connectors. The connectors are be used by Privileged Access Service to reach out to target systems.

Discovering Alternative Accounts

You can use Delinea Privileged Access Service to discover alternative accounts in Active Directory (typically a higher-access or privileged account such an administrative account), associate them with the relevant owner accounts (the non-privileged account), and log-in to the alternative accounts using your non-privileged accounts. For example, system administrators typically have several accounts, a user account for general log-ins and an administrative account to access specific systems and services. You can automatically add these administrative accounts (referred to in general as “alternative accounts”) to Privileged Access Service and we manage the password generation for these accounts. You can then log-in to the administrative account using the general account. Alternative accounts to be discovered and the owner accounts need to be in Active Directory.

The alternative accounts can have permanently-assigned group memberships that grant privilege (e.g. Domain Admins, Local Administrators). These accounts can also use DirectAuthorize for privilege elevation.

The procedures for discovering alternative accounts and Privileged Access Service management of these accounts include:

1. "Creating an alternative account discovery profile"
2. "Assigning alternative accounts profile management permissions"
3. "Running an alternative accounts profile"
4. "Assigning or re-assigning owners for alternative accounts"
5. "Committing alternative accounts"

The **History** page allows you to view activity for previous and current discovery jobs. You can use the History page to learn more about the items added to the Privileged Access Service.

Prerequisites

Before you start creating a profile to discover alternative accounts, make sure you have met the following requirements:

1. The relevant domains must also have administrative accounts configured. See "Setting Domain Admin Accounts" on page 493
2. The domains for which you want to discover the alternative accounts must have the “Enable automatic account maintenance using administrative account” policy enabled (***Resources*** > **Domains** > Select the relevant domain > **Policy**). This policy is required for Privileged Access Service to manage the alternative accounts.
3. The alternative account used to run a service should have automatic password rotation enabled. See "Automating Password Rotation" on page 507 for more information.

Assigning Alternative Account Profile Management Permissions

You can delegate permissions to additional users and roles to manage the profile. Additionally, these users must have the “Privilege Service Administrator” rights to see the Discovery tab. See "Admin Portal Administrative Rights" on page 277 for more information about this administrative right.

For each profile, you can add user management accounts and specify the following permissions:

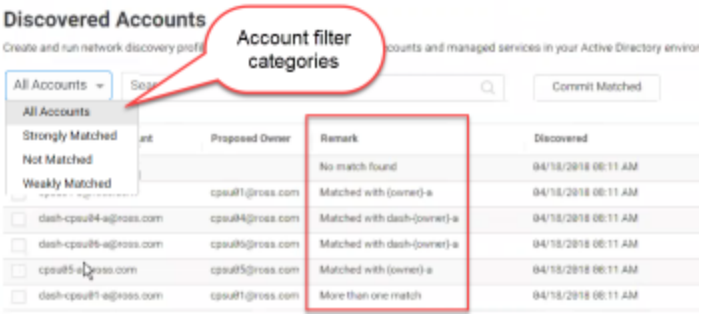
- View – View the profile information only.
- Edit – Edit profile information only.
- Delete – Delete profile information only.
- Grant – Add user management accounts and assign permissions.
- Run – Run the profile.

To add users and assign permissions:

1. Click **Discovery>Alternative Accounts> Profiles**.
2. Select the relevant profile and click **Permissions**.
3. Click the **Add** button.
4. Start typing the user, group, or role in which you want to assign profile management permissions.
5. Select the relevant user, group, or role.
6. Click **Add**.
7. The user is added to the Permissions page with only View permission.
8. Assign the necessary permissions by selecting the relevant check-box.
9. Click **Save**.
10. The specified user now has the specified permissions to manage this profile.

Assigning Owners for Alternative Accounts

After Privileged Access Service discovers the alternative accounts that match your defined username filter, the discovered accounts are listed on the Discovered Accounts page. The accounts on this page have not been added to and are not being managed by Privileged Access Service. They need to be committed before they are added. See "Committing Alternative Accounts" on page 587 You need to review the proposed owners that we have associated with the accounts. Proposed owners are the user accounts that we have found based on the username filter you defined when you created the profile. The “Remark” column shows the username filters we used for matching the accounts to the proposed owners and when no match or multiple matches are found.



It is important that you review the accounts with multiple matches (shown in the Remark column as “More than one match”). Accounts with multiple matches are grouped into the “Weakly Matched” filter category. Accounts with no matches are grouped into the “No Matched” category. Accounts with one match are grouped into the "Strongly

Matched" category. You can assign owners to the accounts that do not have proposed owners or re-assign owners. Detailed information around each category:

- Not Matched – Privileged Access Service could not find an owner to associate with the alternative account. You can manually assign an owner to that account.
- Strongly Matched – Privileged Access Service found only one owner associated with the alternative account. For example, you have the following accounts in Active Directory:

  john01

  john01-a

  admin-john01-a

  The username filter defined in the profile contains two patterns: {owner}-a|admin-{owner}-a

  The john01-a alternative account is matched with only one owner of john01. The admin-john01-a alternative account is matched with only one owner of john01. These matches represent 2 strong matches.
- Weakly Matched – Privileged Access Service found more than one owners associated with the alternative account based on your defined username filter. For example, you have the following accounts in Active Directory: john01@company.com, john01-a@test.com, and john01@test.com

  The defined username filter in the profile is: {owner}-a

  The alternative account john01-a@test.com has two matches of john01@test.com and john01@company.com.

  The discovery will automatically pick john01@test.com as the owner because it has the same domain as the alternative account. However, because there are two matches, this discover is considered weakly matched.

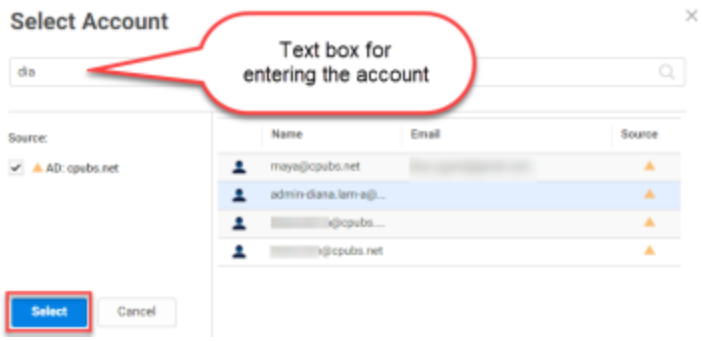
  Privileged Access Service assigns the owner of weakly matched accounts using the following prioritization methods:

  1. Assign the owner from the same domain as the alternative account.
  2. Assign the owner from the same forest.
  3. Sort the log-in name by alphabetical order and assign the first owner in the list.

Note: Accounts in the “Weakly Matched” category must me committed manually. See "Committing Alternative Accounts" on the next page for information on committing accounts.

To assign or re-assign owners:

1. Click **Discovery** > **Alternate Accounts** > **Discovered Accounts**.
2. Select the check box associated with the account for which you want to assign or re-assign an owner.
3. Click **Actions** > **Assign Owner**.
4. Start typing the relevant account name into the text box.
5. Click the correct account name from the list and click **Select**.



The proposed owner is updated and the **Remark** column shows “Explicitly set by user...” to record that you manually assigned the owner. When you are satisfied with the owner association, you are ready to commit

Committing Alternative Accounts

When you are ready for Privileged Access Service to manage the alternative account passwords and bring those accounts into our system, then commit the accounts. Committing the alternative accounts mean you are allowing Privileged Access Service to do the following on the accounts:

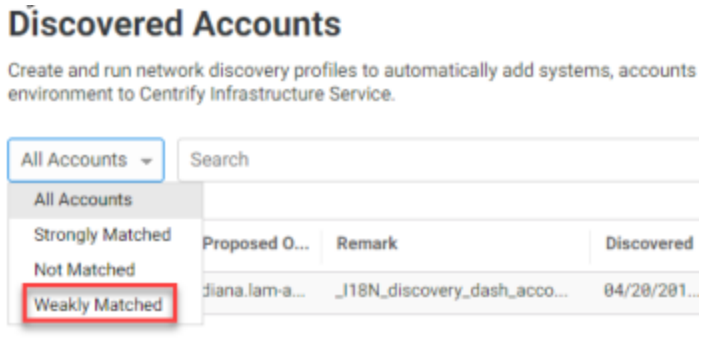
- Add a domain account representing the alternative account.
- Change the account password to a value that only Privileged Access Service knows.
- Grant the associated owner permission to use the account.

Note: The user performing the commit action must have the domain add account permission. If the account is already being manage by Privileged Access Service, then the account must have the Grant permission on the account because so that we can update the permission for all the owners.

You can commit all Strongly Matched accounts by clicking the **Commit Matched** button on the Discovered Accounts page. After you commit an account, it is moved from the Discovered Accounts page to the Accounts page (**Resources** > **Accounts**). Weakly matched accounts must be committed manually.

To commit manually:

1. Click **Discovery** > **Alternate Accounts** > **Discovered Accounts**.
2. (Optional) Use the filter dropdown box to find the weakly matched accounts.

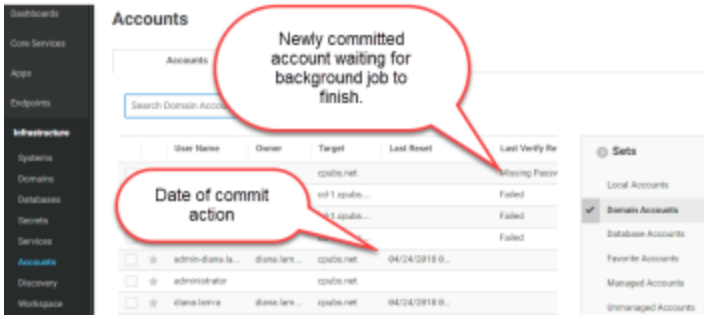


3. Select the check boxes associated with the accounts for which you want to commit.

4. Click **Actions > Commit**.
5. Click **Yes** to confirm the commit.

   The commit process runs in the background. Accounts that fail the commit process contain error messages in the “Commit Result” column. Successfully committed accounts are removed from the Discovered Accounts table. Refresh the page to see the updated discovered accounts.

After you commit the accounts, you can navigate to **Resources > Accounts** to see the successfully committed accounts. The newly committed accounts may show “Missing Password” in the Last Verify Result column until the background job finishes. When the background job finishes, the Last Verify column shows the date and time of the verification and you can now access the alternative account using the general account.



Creating an Alternative Account Discovery Profile

Creating a profile allows you to specify a filter pattern for identifying the alternative accounts in Active Directory. After the profile is created, you can optionally delegate permissions to additional users and roles to manage the profile. See "Assigning Alternative Account Profile Management Permissions" on page 584

To create an alternative account discovery profile:

1. Log in the Admin Portal.
2. Click **Discovery > Systems and Accounts > Profiles > Add Discovery Profile** button.
3. The Settings page opens.

4.
5. Provide the following information on the Settings page:
6. Enter a Name for the profile.

a. (Optional) Enter a profile description.

b. Select Active Directory or Port Scan

   For Active Directory:

   i. Select the domains for which you want to discover the alternative accounts. We search for alternative accounts within the specified domain(s) and Active Directory Organization Units (OUs). We search all the forests that have a Delinea Connector installed (with Active Directory proxy enabled) for the owner accounts.

   ii. (Optional) Select the Active Directory groups within your selected domains to discover the alternative accounts.

   The alternative accounts found in a particular domain are filtered by the Active Directory groups that belong to the same domain.

   For Port Scan:

   i. Fill in the **IP Address**, **Subnet**, and **Range** fields.

   ii. Click **Add** to add new discovery accounts.

7. Click **Save**.

We show the newly created profile with the Ready status in addition the following information on the Profiles page.

Field Name	Description
Last Run	Date and time the profile was run.
Elapsed Time	Time it took to run the profile.
Status	Profiles can have the following statuses: Starting -- You have started the discovery process on the profile. Ready -- Profile is configured and ready for discovery. Discovering Accounts -- Alternative accounts are being discovered. Discovering Owners -- Owner accounts are being discovered. Saving -- Saving the results.

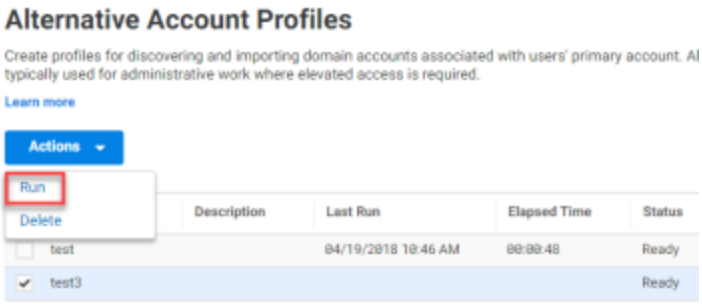
Running an Alternative Account Profile

You run a profile to initiate the discovery process and find the alternative accounts. You can only run profiles that are in the Ready status. There is no limit to the number of times you can run a profile.

Privileged Access Service allows for only one discovery process to be run at a time. If a discovery is running while another user tries to start it, the second user receives an error message.

To run a profile:

1. Click **Discovery** > **Alternate Accounts** > **Profiles**.
2. Select the check boxes associated with profiles you want to run.
3. Select **Run** from the Actions drop-down list.

4. 

5. The status changes to Starting while Privileged Access Service scans your network for the alternative accounts.
6. Refresh the Profiles page to verify that discovery is done.

   The status changes to Ready when discovery is done.

Discovering Systems

You can automatically populate Privileged Access Service with computers, network devices, and accounts by creating discovery profiles and running discovery jobs. Discovery profiles describe the type of information you want to discover– Windows and UNIX computers, servers, and workstations only or network devices as well. You can define a profile to use the following discovery methods:

- Active Directory method - Scans only Active Directory joined systems (Windows and UNIX workstations and servers).
- Port scanning method - Scans network devices (for example routers) and UNIX/LINUX/Windows system that are not joined to Active Directory, in addition to the Active Directory joined systems.
- EC2 discovery method - Scans AWS EC2 instances and optionally enrolls the system with the Delinea Client.

By default, discovery jobs ignore previously discovered systems that have been deleted to avoid rediscovering the same objects. The deleted systems are listed in **Discovery** > **Excluded Systems** in the Systems area. You can remove systems from this list if you want them to be rediscovered.

The **History** page allows you to view activity for previous and current discovery jobs. You can use the History page to learn more about the items added to the Privileged Access Service.

Note: Passwords for discovered accounts on domain-joined Windows systems do not need to be manually updated if system and domain policies are configured for local account password reconciliation. See "Configuring Windows local account reconciliation", for configuration details.

Port Scanning Discovery

Port scanning includes two levels of discovery:

1. Basic discovery -- Privileged Access Service first probes a few well-known ports to determine the basic system type - generic SSH or windows.
2. Detailed discovery -- Then we use the specified discovery account to run a detailed discovery. This discovery gets more system information, such as the accounts associated with application pools, services, and scheduled tasks. The detailed discovery requires that you specify an account with local administrative rights when you create the profile. See "Adding accounts for port scan discovery."

The procedures for a port scan discovery include:

1. "System discovery pre-requisites"
2. "Adding accounts for port scan discovery"
3. "Creating a port scan discovery profile"
4. "Specifying systems discovery actions"
5. "Running a systems discovery job"
6. "Assigning systems profile management permissions"

Active Directory Discovery

The discovery profile account you specify must have sufficient permissions to perform computer, domain, service, and account discovery. At a minimum, the discovery profile account must have:

- Read permissions on the domains to be discovered
- Local administrator permissions on computers to be discovered – If it does not have local administrator permissions, then you can discover only basic system information (such as the system type).

The procedures for an Active Directory discovery include:

1. "System discovery pre-requisites"
2. "Creating an Active Directory discovery profile"
3. "Specifying systems discovery actions"
4. "Running a systems discovery job"

EC2 discovery

EC2 discovery imports AWS EC2 instances into Privileged Access Service as systems. Optionally, you may enroll the system to the discovered system using the Delinea Client, and auto-configure the Use My Account feature and Linux sudo privileges.

The procedures for an EC2 discovery include the ability to:

- "Use security automation for EC2 instances on AWS"
- "Assign systems profile management permissions"
- "Run a systems discovery job"
- "View discovered system information"
- "Modify systems discovery profiles"
- "Delete discovered objects"
- "Delete a systems discovery profile"

Adding Accounts for Port Scan Discovery

Discovery accounts are used for accessing the systems you want discovered through port scanning. These accounts must have sufficient permissions to perform network device, computer, domain, service, and account

discovery. You can add a local admin account or account that is SSH key-created and domain accounts from this page (for use during the profile creation process) or add them ad hoc during the profile creation process. Domain accounts you add here cannot be managed accounts because you must specify the account password. See "Using Managed or Unmanaged Accounts" on page 477 for information about managed accounts. If you want to add a managed domain account for use during discovery, then add it ad-hoc during the profile creation process.

A detailed discovery (to get more detailed information, such as the accounts associated with IIS application pools, services, and scheduled tasks), requires one of the following:

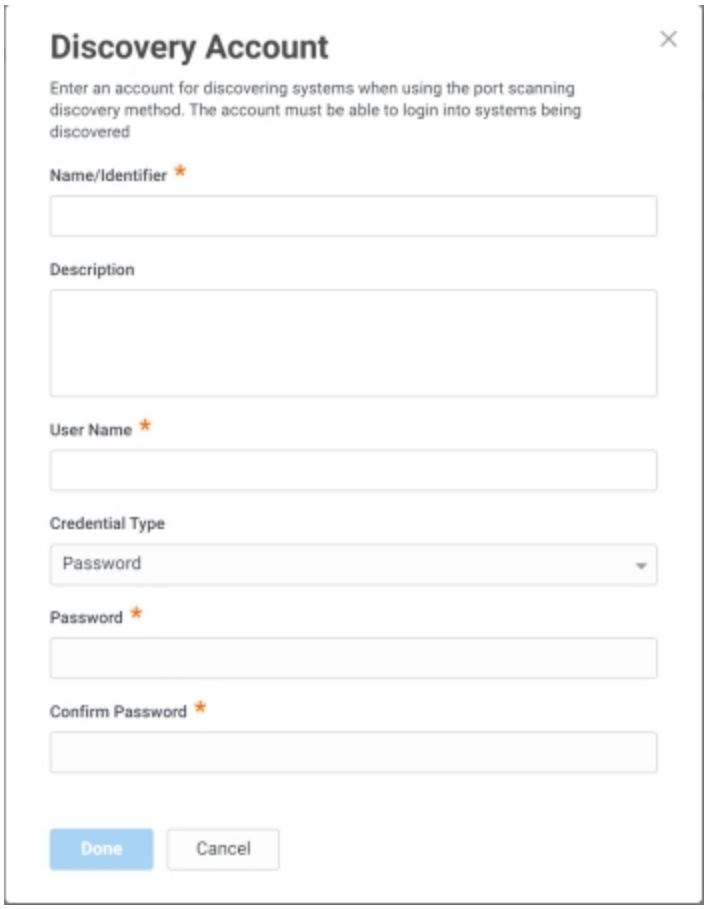
- You specify an account with local administrative rights or account that is SSH key-created.
- You specify domain accounts that are local domain administrators or domain admin groups that have local administrative rights on each of the domain-joined Windows systems.
- You specify an account that is SSH key-created.

If you run port scan discovery without local administrative rights or with a domain account that does not meet the above requirement, then Privileged Access Service can only perform a basic discovery -- discover only the system type (UNIX/LINUX system or Windows system). When you add the account on this page, it becomes available for selection during the profile creation process.

For information about adding SSH keys, see "Adding SSH keys" on page 512

To add a discovery account:

1. Click **Discovery > Systems and Accounts > Discovery Accounts**.
2. Click the **Add Account** button.



3. Enter a unique Name/Identifier for this account.
4. This name cannot already exist as a discovery account name/identifier.
5. Enter the account **User Name**.
6. Choose a password or SSH key.
7. Enter the account **Password**.
8. Confirm that you have entered the password correctly. An incorrect password entry will increment the Windows password counter by one each time you run discovery.
9. Click **Done**.

Assigning Profile Management Permissions to Systems

You can delegate permissions to additional users and roles to manage the profile. Additionally, these users must have the “Privilege Service Administrator” rights to see the Discovery tab. See "Admin Portal Administrative Rights" on page 277 for more information about this administrative right.

For each profile, you can add user management accounts and specify the following permissions:

- View – View the profile information only.
- Edit – Edit profile information only.

- Delete – Delete profile information only.
- Grant – Add user management accounts and assign permissions.
- Run – Run the profile.

To add users and assign permissions:

1. Click **Discovery> Systems and Accounts** >**Profiles**.
2. Select the relevant profile and click **Permissions**.
3. Click the **Add** button.
   a. Start typing the user, group, or role in which you want to assign profile management permissions.
   b. Select the relevant user, group, or role.
   c. Click **Add**.
   d. The user is added to the Permissions page with only View permission.
4. Assign the necessary permissions by selecting the relevant check-box.
5. Click **Save**.
6. The specified user now has the specified permissions to manage this profile.

Automatically Discover Servers and Workstations

After you log on, you can expand Infrastrcuture, then click **Discovery** to automatically discover computers and accounts based on the criteria you specify. For example, you can select options such as Windows Server or UNIX Server to create a discovery profile and run a discovery job. The discovery job will scan the Active Directory domains and organizational units you select to collect information about the servers and workstations on your network and any services you have configured to run under local or domain accounts. For more information about creating discovery profiles and running discovery jobs, see "Discovering systems."

If you want to skip the discovery scan of your network, however, you can also get started with Privileged Access Services by manually adding systems, domains, databases, services, and accounts.

Automating Security for EC2 Instances on AWS

You can discover and automate privilege management based on policies.

Discover and maintain inventory for VMs

For cloud infrastructure and cloud identity owners, this feature helps you discover and maintain the inventory for all VMs running on AWS cloud service providers.

In Privileged Access Service:

- You can see all the VMs running on various different Cloud Service Providers.
- The inventory is updated if a new VM is created or an existing VM is deleted from the cloud service provider.

Use SSO for Cloud VMs

IT admins or Cloud Ops engineers can use their enterprise identity (For example their AD user credentials) and their favorite native client application to log into to the VMs running on the cloud infrastructure without using a shared local account.

With Privileged Access Service you can define which users:

- Have remote access to specific VM machines
- Can run privilege commands on specific VM machines.

An auditor can also discover who has remote access to VM machines running on the cloud.

Users can login to their authorized VMs using their on-premise enterprise identity, on Windows or Mac with their favorite native SSH client application such as Putty, SecureCRT, RoyalTS, mRemoten, or RDP client application.

Examples

You have the following:

- EC2 instances deployed into AWS
- 4 accounts with multiple regions
- AWS accounts you do not manage
- One VPC per region per account, 200 systems total:
  - Each of the 5 regions has 20 VPCs
  - Each VPC has 10 instances (5 Windows, 5 Linux)

You can set up all your EC2 instances with Delinea Client enrolled systems. This enables your admins to login using Use My Account, and enables you to remove Linux SSH key access.

Set up IAM Accounts

Creating an Administrative IAM Account

You need an IAM for each AWS account you plan on discovering. If you don't have one already, create an administrative IAM credential for your use, or ask someone to do this for you. We recommend your IAM name matches your company's e-mail address.

Note: The use of root credentials is highly discouraged.

See "Adding IAM User Accounts" on page 569 for more information.

Creating a Discovery IAM Account

You can use your administrative IAM when doing discovery, but a better practice is to create a separate discovery IAM that has just enough privileges for discovery. You need to create a new IAM policy for discovery, and add a new discovery IAM with the policy attached.

To create a new IAM policy and attach it to a new discovery IAM:

1. Go to the IAM console in AWS.
2. Click the **Create Policy** button and select the **JSON** tab.
3. Replace the policy text with the following:

   "Copy"

```
{
    "Version": "2012-10-17",    "Statement": [        {            "Effect":
"Allow",            "Action":
[               "iam:GetUser",               "iam:ListAccountAliases",
 "iam:ListInstanceProfiles",               "iam:PassRole",               "ec2:Authori
zeSecurityGroupIngress",               "ec2:CreateSecurityGroup",               "ec2:
CreateTags",               "ec2:Describe*",               "ec2:GetPasswordData",
           "ec2:RunInstances",               "ssm:GetCommandInvocation",
  "ssm:SendCommand",               "sqs:DeleteMessage",               "sqs:ReceiveMes
sage"            ],            "Resource": "*"        }    ]}
```

4. Click **Review Policy** .
5. Name the policy **CompanyDiscoveryPolicy**.
6. Click **Create Policy**.
7. Create an IAM user with your user's company email address. For example, discovery@company.com.

   Note: Ensure you allow API access and save the access key and secret to your desktop.

8. On the **Permissions** tab for your IAM, click **Add Permissions** .
9. Click **Attach existing policies directly**.
10. Filter the policies by your company name and check **CompanyDiscoveryPolicy**.
11. Click **Review and Add Permissions**.

Configuring EC2 Discovery

Importing AWS Key Pairs

PAS needs the private key pairs for your instances for login. For each of your key-pairs, add them to **Resources / SSH Keys**.

Configuring PAS Roles

EC2 discovery profiles optionally reference a number of Privileged Access Service roles.

Create the following roles:

Name	Description
Delinea Client Auth Users	Users in this role are permitted to login to systems enrolled via Delinea Client.

Name	Description
Delinea Client for LinuxAdministrators	Users in this role are granted full sudo permissions on systems enrolled via Delinea Client.
Centrify Client for Windows Administrators	Users in this role are granted full Administrators access on systems enrolled via Centrify Client.

EC2 discovery optionally enrolls the discovered EC2 instances. Additionally, it configures Use My Account for Linux instances and gives your Delinea Client for Linux Administrators roles full sudo permissions. Add members to this role to grant them access.

Configuring Sets

EC2 discovery can optionally add discovered systems and accounts to sets. For example, creating manual sets similar to the following:

- Discovered systems
- Discovered systems without credentials
- Discovered local accounts

Creating Cloud Providers

For each target discovery account a cloud provider must be created. See "Create a discovery IAM account."

Create a Discovery Profile

To add a discovery profile:

1. In the Admin Portal navigate to **Discovery** > **Systems and Accounts** > **Profiles**.
2. Click **Add Discovery Profile**.
3. Choose a discovery method. For example, **AWS EC2 Instances**.
4. Enter the discovery profile **Name** and optional **Description** and click **Next**.
5. Each discovery profile requires a minimum of one Discovery Scope. A scope identifies which instances you want discovered.

   Note: Use the **Delete** button next to a scope if you need to delete an existing scope.

   To add a discovery scope:

   Note: You will need a cloud provider to create a new scope. For more information see "Create cloud providers."

   a. Click **Add** to create a new scope.

   b. Select a cloud provider.

c. Under **Credential to use for selected cloud provider**, choose a credential to use with the cloud provider and click **Next**.

d. Select at least one data center. For AWS, this list displays the available AWS regions.

> **Note:** You can select VPCs and/or subnets. To see VPCs and subnets, click the **+** icon next to a region and/or VPC.

You can optionally set the following by using the selection options under their associated columns:

- FQDN (Fully Qualified Domain name)
- Proxy
- System Type
- System Name

e. Click **Next**.

f. Add at least 1 SSH key pair. Use the **Upload** button or the drag-and-drop window to upload a new key pair or click **Choose** to select an existing one.

g. Click **Done**.

6. Click **Next**.
7. Enter the following information:
   - Enrollment Options
   - Additional Action

> **Note:** Enrollment of Windows systems requires the systems to be managed with AWS Systems Manager.

8. Click **Next**.
9. (Optional) Click **Add** to add a new monitor setting and click **Next**.
10. (Optional) Click **Add** to add a new scheduling setting and click **Next**.
11. (Optional) Click **Add** to add a new permission setting and click **Next**.
12. Click **Done**.

Configuring a Discovery Profile for EC2 State Monitoring

You may optionally configure your discovery profile to monitor EC2 state changes and automatically incrementally add or delete systems without having to wait for the next discovery "run".

To do this, you must first configure the following:

- SQS queue used to receive the stage change events
- CloudWatch rule to send state change events to the queue.

To configure an SQS queue:

1. Go to the SQS AWS console.
2. Click the **Create Queue** button.
3. For **Type of queue** select **standard**.
4. For **Name**, enter **ec2_state_events** or choose a custom name.
5. Leave the remaining fields with the default settings.
6. Once the queue is created, remember the queue URL which will look similar to `https://sqs.us-west-1.amazonaws.com/215634055688/ec2-state-events`. You will need this information for the CloudWatch rule.

To configure an Amazon Event Bridge Rule:

1. Go to the Amazon Event Bridge Console.
2. Create an Amazon Event Bridge rule called ec2-state-watcher
3. Navigate to **Events** > **Enter Rules**
4. Select the default Event bus and set the Name to ec2-state-watcher.

   Note: You can leave the **Description** blank.

5. Click **Create Rule**.
6. In the **Event Source** section, click the **Edit** button to display the **Event Pattern Preview** page.
7. Set the following information:
   a. **Event pattern**: enabled
   b. **Pre-defined pattern by service**: enabled
   c. **Service Provider**: AWS
   d. **Service Name**: EC2
   e. **Event Type**: EC2 instance state-change notification
   f. **Specific states**: running, terminated, stopped
   g. **Any instance**: enabled
8. Insert the following text:

```
{
  "source": [    "aws.ec2"  ],  "detail-type": [    "EC2 Instance State-change
Notification"  ],  "detail": {    "state":
[      "running",      "stopped",      "terminated"    ]  }}
```

9. Select **Event bus** and set **AWS default event bus** to enabled
10. Select **Targets** and set:
    a. **Target** to **SQS queue**.
    b. **Queue** to the name of your SQS queue

11. In the dropdown, select **SQS queue**.
12. For the select queue dropdown, choose the SQS queue you created.

Auto-Deployment from AWS Cloud using a Connector

In order to establish an SSH or RDP session to your discovered instances, you need one or more connectors that have connectivity to the instances. There are a number of network topologies you can use to meet this requirement. The most common methods are:

- Deploy connector(s) into each VPC where you have instances.

  The connector needs to have outbound connectivity, but does not require inbound connectivity.
- Deploy a connector on-premise and establish VPN(s) from the connector to reach your discovered instances.

Once you've established connectivity to the instances, you have the option to deploy a connector manually, but it's much simpler and more efficient to use the wizard to deploy a connector.

To deploy a connector:

1. In the Admin Portal, click **Resources** > **Cloud Providers**.
2. Right-click on a cloud provider **Name** to open the dropdown and choose **Deploy Connector**.
3. Select an **IAM User** and **Region**. This will display the VPCs in the selected region for the IAM user account.
4. Select a **VPC** and specify an **AMI ID**.
5. Select a **Subnet**.
6. Optionally select an **IAM Role** for the instance. For example, you can choose a role that will enable the AWS system manager.
7. Enter a custom **Instance Name**.
8. Choose a **Security Group** or create your own security group.
9. Choose a **KeyPair** which will be used to launch the instance.
10. Click **Deploy Connector**.

Once the setup is complete, the system will reach out to AWS and create the instance.

Note: In AWS can will be able to see the pending status under Instances. It will take a few minutes to create, spin up, and deploy the instance. During this process, the system reaches out to AWS, downloads the installer, install the software and any required dependencies, reboots, etc.

Note: As part of the connector registration, Delinea PAS sets up a Resource Connector Mapping. This is used to route traffic through a connector when establishing sessions to the discovered systems. The connector is then used to surface that VPC.

To see the connector mappings, navigate to **Settings** > **Resources** > **Resource Connector Mappings**.

In the table, you can see the connector(s) used for each VPC. If desired, you can modify the connectors used to reach the VPC.

Note: When aconnector is deployed to a VPC, this information is set it up automatically.

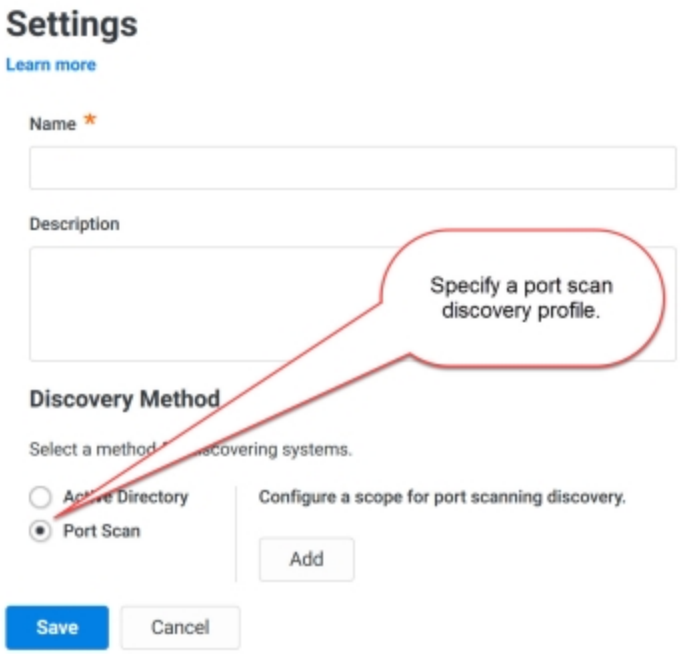
A connector can be added if it's on premises, but the VPC mapping will need to be applied manually.

Creating a Port Scan Discovery Profile

Port scanning probes your specified system and uses the defined account credentials to log-in to the system and determine the system type (IBM i, HP NonStop OS, Windows computers, servers, etc.). If you do not specify an account or specifies one with insufficient permissions, the Privileged Access Service can only do a basic discovery. See "Adding Accounts for Port Scan Discovery" on page 591 for more information about the discovery accounts.

To create a port scan system profile:

1. Click **Discovery > Systems and Accounts > Profiles**.
2. Click the **Add Profile** button.
3. Enter a name for the profile.
4. (Optional) Enter a description for the profile.
5. Select **Port Scan** in the discovery method area.



6. Click the **Add** button associated with the "Configure a scope for port scanning discovery" area.
7. The “Discovery Scope” window opens.
8. a. Enter either an IP address, subnet (in CIDR format), or IP address range.
   b. Port scanning identifies the connectors for discovery based on the system subnet mapping you have configured on the **Admin Portal > Settings >Resources> System Subnet Mapping** page. If you do not specify any subnets, then Privileged Access Service uses all connectors by default. Contact Delinea Support to specify the use of specific connectors without configuring system subnets.
   c. (Optional) Click the **Add** button to select an existing account to be used for port scanning.

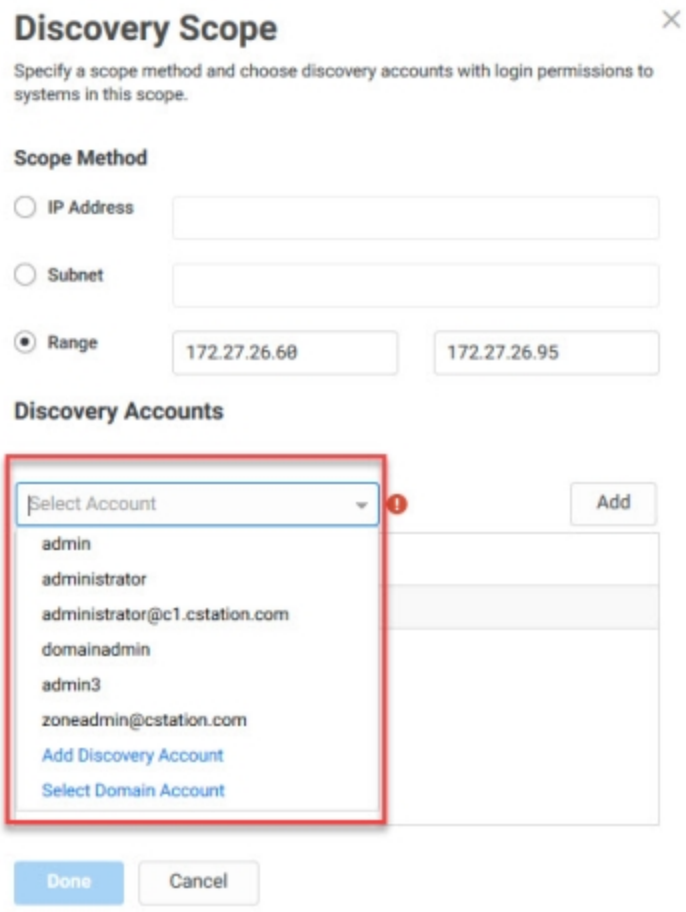
d. If you have added the accounts using the **Discovery > Discovery Accounts** option in the System area, then you will see them in this drop-down list.

e. Alternatively, you can specify a discovery account or a domain account ad hoc by selecting **Add Discovery Account** or **Select Domain Account** from the drop-down list. The domain account you specify here can be a managed account. See "Using Managed or Unmanaged Accounts" on page 477 for more info on managed accounts.

f. A detailed discovery (to get more information, such as the accounts associated with IIS application pools, services, and scheduled tasks), requires one of the following credentials:

g.
- You specify an account with local administrative rights.
- You specify domain accounts that are local domain administrators or domain admin groups that have local administrative rights on each of the domain-joined Windows systems

h. If you run port scan discovery without local administrative rights or with a domain account that does not meet the above requirement, then Privileged Access Service can only perform a basic discovery -- discover only the system type (UNIX/LINUX system or Windows system).



i. Click the associated **Add** button.

j. Click **Done**.

9. Select the system types you want the discovery to find.
10. The default is to discover all system types (Windows Computers, Unix Computers , IBM i, and HP NonStop OS) and Network Devices selected.
11. (Optional) Select the **Import systems detected without known credentials** check box if you want Privileged Access Service to discover and import systems even if the required credentials are not provided.
12. (Optional and only available if you enable the above check box) Select the **Ignore if system name not found in DNS** check box if you want Privileged Access Service to **not** discover and import the systems whose names are not found in DNS.
13. (Optional) Specify the default DNS domains by clicking the Add button associated with the “DNS Suffix Search List” field.
14. These domains are used to find the fully qualified domain name (FQDN) in the DNS. Privileged Access Service logs-in to the system to discover the system name, type, and FQDN. If a system does not report on its FQDN, Privileged Access Service uses this list to find the FQDN in the DNS.
15. Click **Save**.

You can now specify the actions you want performed as part of the discovery.

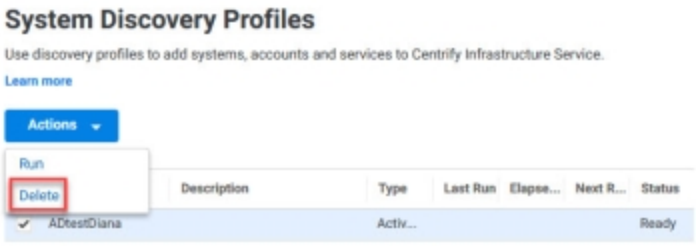
Deleting Discovered Objects

You can delete any previously discovered network devices, computer, domain, service, or account by selecting it, then clicking **Delete** from the Actions drop-down list. If you manually delete a discovered object, however, the object will not be added to Privileged Access Service the next time you run a discovery job by default. Privileged Access Service handles the re-discovery of previously deleted systems, domains, services, or accounts differently. Previously deleted systems or accounts are listed on the Excluded Systems or Excluded Accounts page in Admin Portal > **Discovery** > **Systems and Accounts** > **Excluded Systems** or **Excluded Accounts**. If you want previously deleted systems or accounts to be re-discovered next time you run a discovery job, then remove those systems or accounts from the Excluded Systems or Excluded Accounts page.

If you accidentally delete a discovered domain, service, or account , you can manually add it to Privileged Access Service or run a discovery profile with the relevant Windows Services options selected and the **New and existing systems** option selected on the Actions page -- Admin Portal > **Discovery** > **Systems and Accounts** > **Profiles** > relevant profile > **Actions**. Domains, services, and accounts are tied to services or tasks, which are tied to systems. If you have not deleted the associated systems, then re-running a discovery job will re-discover those previously deleted domains, services, or accounts -- provided you have the relevant options selected on the Actions page. See "Specifying Systems Discovery Actions" on page 610 for more info on the actions.

Deleting a Systems Discovery Profiles

You can delete any previously-defined discovery profile by selecting it in the list of profiles, then select **Delete** from the Actions drop-down list. You are prompted to confirm the deletion.



Creating an Active Directory Discovery Profile

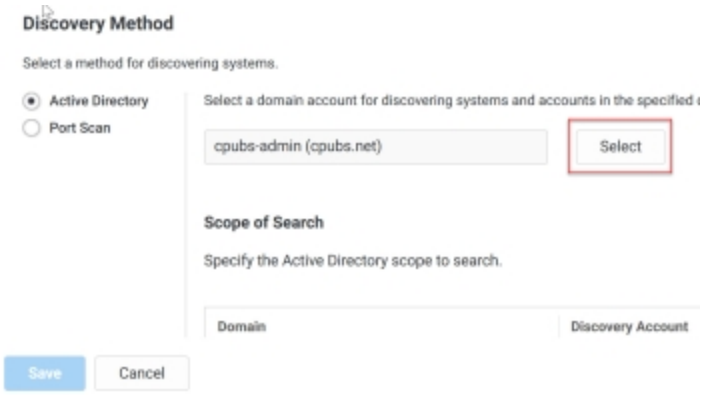
You create an Active Directory discovery profile to probe Windows and UNIX computers, servers, and workstations. A discovery profile identifies the type of systems you want to locate on your network and add to the Privileged Access Service. After you configure the details for the discovery profile, you can use the profile to run a discovery job immediately or schedule the discovery job.

You can also create multiple discovery profiles to look for computers, domains, services, and accounts that match different criteria. For example, you might create separate discovery profiles to look for Windows servers and UNIX workstations.

Active Directory discovery uses the connectors specified on the Admin Portal > **Resources** > **Domains** > select the relevant domain > **Connectors** page.

To create an Active Directory discovery profile:

1. Log in to Admin Portal.
2. Click **Discovery > Profiles** in the Systems area.
3. Click **Add Profile** and type a unique name for the new discovery profile.
4. Type an optional description for the profile.
5. Confirm that the **Active Directory** is selected for the discovery method.
6. Click the **Select** button to select the domain account for discovering systems and accounts in the specified domains.



7. The Select Account window opens.

8. a. Start typing part of the account name to search for and select an existing account with read permissions and local administrator permissions on the computers to be discovered.
   b. The account you specify must have the Privileged Access Service Administrator administrative right to successfully discover computers, domains, services, and accounts on the network.
   c. Click the **Select** button at the bottom of the window.
9. Review the list of domains to be searched and select at least one domain.
10. The discovery profile displays the domains and sub-domains found in Active Directory as candidates for discovery. Only domains that are automatically synced with an active connector are available for discovery.

11. (Optional) Click **Add** in the Group Membership area to specify the Active Directory group in which you want to discover.
12. Review the list of filter options and modify the filters to be used as needed.
13. For example, if you only want to discover Windows servers, you would select the **Windows Computers** and **Servers** filters. For Windows computers, the operatingSystem attribute determines whether the computer is a server or workstation. If you are discovering UNIX and Linux computers joined to the domain, the Delinea license type determines whether the computer is identified as a server or a workstation.
14. Note that only computers that are active—with a computer account password that has been changed in the last 14 days—are candidates for discovery. Computers objects that are disabled or inactive are ignored.
15. Systems already imported are not overwritten on subsequent discoveries.
16. Click **Save**.

Modifying Systems Discovery Profiles

You can modify any previously-defined discovery profile by selecting it in the list of profiles. You can then make changes to any of your previous selections. For example, you might want to change the user account that runs the discovery job or reconfigure the profile to use Active Directory or port scan method.

Port Requirements for IIS Applications Pools

Be sure the following ports are open on the IIS server to allow discovery of IIS application pools and related accounts:

- Port 135 (TCP) for inbound communication with the RPC endpoint mapper program.
- A custom inbound firewall rule to allow communication for the DllHost.exe process on all RPC Dynamic Ports.
- Port 139 (TCP) for file and printer sharing (NB-Session-In) inbound communication if the operating system is Windows Server 2016.

For more information about configuring firewall rules for discovery, see "System Discovery Prerequisites" on the next page

Running a Systems Discovery Job

You run a profile to initiate the discovery process. You can put the discovery job on an automatic run schedule or run the discovery job manually. You can only run one discovery job at a time. A user must have “Run” permission for the profile to run discovery. A user must have "Run" and "Edit" permissions for the profile to set up an automatic run schedule.

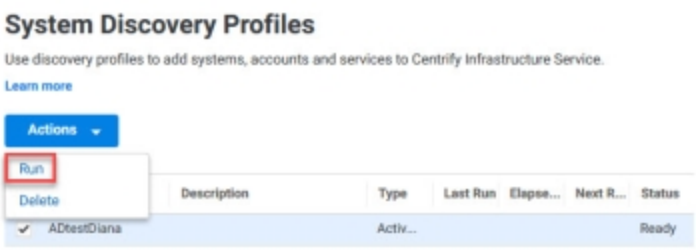
After a successful discovery job is completed, the new systems, domains, computers, and accounts are listed under the appropriate tabs within Admin Portal. If a discovered system already exists in Privileged Access Service and the profile has "Apply Actions to New and Existing Systems", the system is updated. Other existing discovered objects are left unchanged by the discovery process.

Manually Running a Discovery Job

You can initiate a discovery manually.

To run a discovery job manually:

1. In the Admin Portal, click **Discovery** > **Systems and Accounts** > **Profiles**.
2. Select the check box associated with profile you want to run.
3. Select **Run** from the Actions drop-down list.



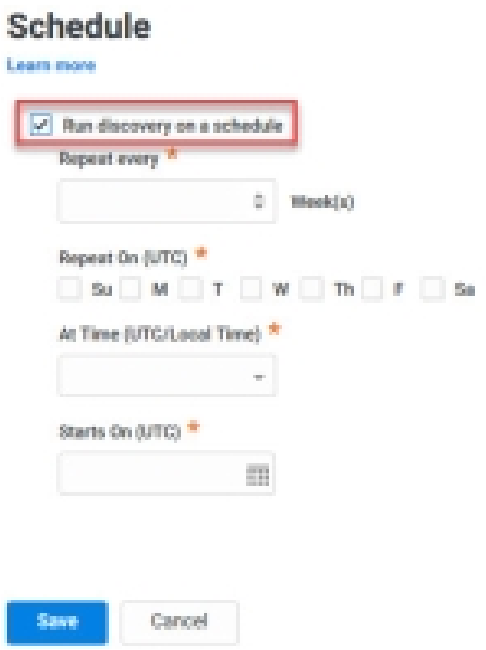
4. The status changes to Running while Privileged Access Service scan your network.
5. Refresh the Profiles page to verify that discovery is done.
6. The status changes to Ready when discovery is done.

Scheduling a Discovery Job

You can schedule discovery to run during a low traffic time period.

To schedule a discovery job:

1. In the Admin Portal, click **Discovery** > **Systems and Accounts** > **Profiles**.
2. Select the profile for which you want to configure a discovery schedule.
3. Click **Schedule**.
4. Enable the check-box associated with “Run discovery on a schedule”.



5. Enabling this option makes the related configurations available.
6. a. Specify how frequently you want the discovery job to run (every week, every two weeks, etc.)
   b. Specify the days of the week you want the discovery job to run.
   c. Specify the time (on the hour) you want the discovery job to run.
   d. Specify the date on which you want the scheduled discovery to start.
7. Click **Save**.

System Discovery Prerequisites

The following are parts of system discovery pre-requisites:

- "Active Directory discovery requirements"
- "Port scanning discovery requirements"
- "Additional Windows discovery"

Active Directory Discovery Requirements

The first phase of the Active Directory discovery method looks for systems that are joined to Active Directory. Typically these are Windows systems but there may be Unix systems as well (requirements for Unix systems are detailed below). The target systems do not need to be online for this first phase of discovery and no special requirements are needed.

Active Directory Discovery Requirements for UNIX

UNIX systems are joined to Active Directory with the Delinea Authentication Service. A Server Suite Agent must be installed on the UNIX system. That agent is used to join the AD/LDAP for discovery when finding Unix systems.

Systems are discovered by performing LDAP queries to Active Directory.

Port Scanning Discovery Requirements

The first phase of the Port Scanning discovery method is done by checking for open TCP ports on a target system. The systems must be online and the systems may or may not be joined to Active Directory. Once open ports are found, attempts are made to connect to the system. By default, one of the specified discovery accounts must be able to authenticate to the target system.

For Windows systems, read-only remote registry access is required along with the following:

- Open firewall.
- Ensure remote registry service is running.
- Group Policies.
- Discovery account must be a local admin.

  Note: One way to achieve this for systems that are joined to Active Directory is to use a discovery account that is a member of Domain Admins.

- The Delinea Connector you use for discovery through port scanning must be on version 18.6 or newer. By default, all connectors are used for discovery. Contact Delinea Support to specify the use of specific connectors for discovery.
- Port scanning requires IPv4 addresses.

For Unix and other systems that have SSH enabled, there are no special requirements. By default, systems that have no known connection credentials are ignored. However, if the "Import systems detected without known credentials" and "Ignore if system name not found in DNS" options are selected, a successful DNS reverse lookup on the system's IP address is required to add the discovered system.

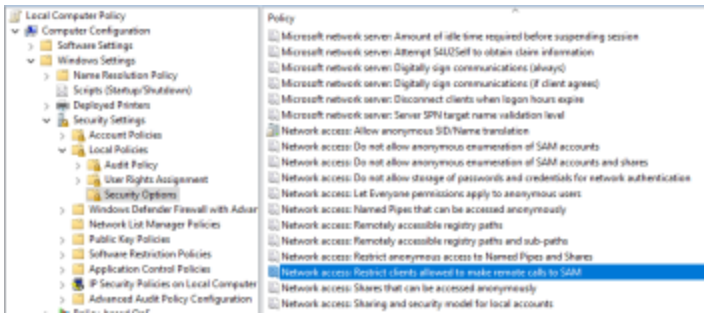
Additional Windows Discovery

For either the Active Directory or Port Scanning methods of discovery, the second phase of discovery may optionally be configured to find additional information about Windows systems:

- Discovery of local accounts.
- Discovery of Windows services, scheduled tasks, and IIS Application Pools along with their associated accounts.

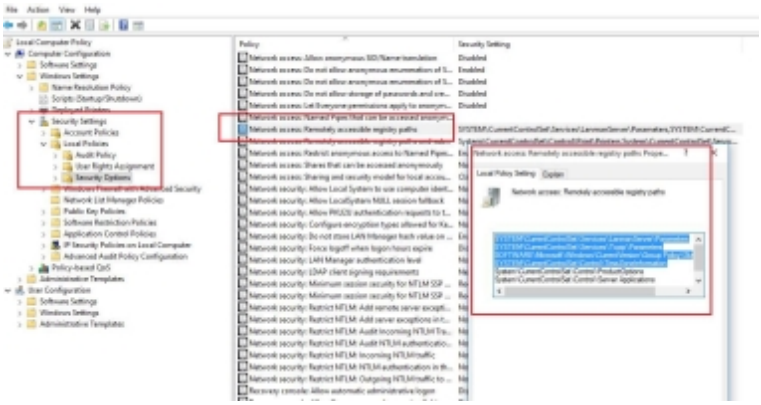
Discovery of Local Windows Accounts

To discover local accounts on a remote machine, the discovery engine needs to make remote calls to the Security Account Manager (SAM) database of the target system. On Windows desktop systems such as Windows 10, the discovery account may not have such permissions by default and you may need to update the Local Security Policy to enable this access. The specific policy setting is located under **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options** > **Network access: Restrict clients allowed to make remote calls to SAM**.



Delinea recommends that you either add the discovery account to this list by clicking the "Edit Security...." button or add the "Authenticated Users" group to this list.

The following requirements are specific to Windows:

1. As part of the detailed discovery, Privileged Access Service reads the following registry locations:
2. HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\ParametersHKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\MachineHKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
3. To remotely read these registry locations from the target machine, confirm the following:
   a. The "Remote Registry" service must be enabled on the target system.
   b. Certain firewall ports must be opened for the remote registry read to work properly. You can typically add a Windows firewall exception for the "Remote Service Management" group to achieve this.
   c. The first four registry keys referenced above must be added to the list of "remotely accessible registry paths" using either the local or domain group policy that applies to the target machine.
   d. 
4. In general, you need to have local administrative privileges to remotely read registry from a system. However, you can work around that by enabling certain Group Policy settings that will allow remote access to the registry paths specified in the third pre-requisite.
5. Since it may not be possible to manually enable the "Remote Registry" service or add firewall exception to each of the systems, you can bulk-apply these settings through group policy.

6. The discovery account must have local administrative rights on each of the systems being probed for Privileged Access Service to perform a detailed discovery (discover services, scheduled task, and IIS application pools).
7. Additionally, the firewall rules named “Remote Service Management” and “Remote Scheduled Tasks Management” must be enabled. If you do not have these rules enabled, you cannot perform a detailed discovery on the target system.
8. In addition to the pre-requisite for running a detailed discovery, discovering IIS application pool requires a few specific ports configurations. See "Port Requirements for IIS Applications Pools" on page 605

A detailed discovery allows you to get more detailed information, such as the accounts associated with IIS application pools, services, and scheduled tasks.

Discovery of Windows Services, Scheduled tasks, and IIS Application Pools

To discover Windows services, scheduled tasks, and IIS application pools, perform the following steps.

" To open a port for discovering scheduled tasks:"

" To open a port for discovering IIS application pools:"

Discovery of UNIX Local Accounts

For either the Active Directory or Port Scanning methods of discovery, the second phase of discovery may optionally be configured to find local accounts on the system. The discovery account must be able to login to the target system and does not need to be a privileged account.

Specifying Systems Discovery Actions

You can specify additional actions you would like Privileged Access Service to perform as part of the systems discovery job. For example, you can specify the Windows services you want discovered and other set related actions. These actions apply to both port scanning and Active Directory discovery.

To specify the actions:

1. Click **Discovery > Systems and Accounts > Profiles**.
2. Select the profile for which you want to specify the actions.
3. Click the **Actions** tab.
4. Select the **Discover Local Windows and Unix Accounts** check box to have Privileged Access Service discover local accounts for Windows and Unix systems.
5. Enabling this check box allows Privileged Access Service to use SSH to log in to a Unix system and discover local accounts. For Windows systems, enabling this check box allows us to use an API call to identify the local accounts and determine if they are privileged account or not.
6. After enabling this check box, you can select the following additional actions:

Action	Description
Manage discovered accounts (domain joined systems only)	Specify that discovered accounts are automatically taken under management. The account system must be domain joined and the domain must have a configured domain administrative account in the domains **Advanced** tab.
Add discovered Windows privileged local accounts to set	This action is specific to Windows accounts. Privileged accounts for Windows systems means they are a member of the local administrator group.Specify the account set to which you want to add the discovered systems without known credentials. Sets are logical groupings of items (systems, databases, etc.) that allow you to specify additional access to the discovered systems and accounts. For example, you can further grant access to discovered systems using the set-level permissions. You must first create a set before you can use it here. See "Adding System Sets" on page 536 to create a system set. Permissions for these sets must be specified before running the discovery job.
Add other discovered local accounts to set	Specify the account set to which you want to add the discovered systems. Sets are logical groupings of items (systems, databases, etc.) that allow you to specify additional access to the discovered systems and accounts. For example, you can further grant access to discovered systems using the set-level permissions. You must first create a set before you can use it here. See "Adding System Sets" on page 536 to create a system set. Permissions for these sets must be specified before running the discovery job.
Limit local account discovery to specific account names	You can select a particular system type. If left empty, discovery will operate on all local accounts. A comma or semicolon separated list of account names can be entered for a system type.

7.

8. Select the **Discover Windows Services** you want discovered.
9. The default is to discover services, scheduled tasks, and IIS application pools.
10. Enable the **Additional Actions** you want taken as part of this discovery job.

Action	Description
Add discovery account as a system local account	The local discovery account used to probe the system is added to the system as a local account.
Add discovered systems to set	Specify the system set to which you want to add the discovered systems. Sets are logical groupings of items (systems, databases, etc.) that allow you to specify additional access to the discovered systems and accounts. For example, you can further grant access to discovered systems using the set-level permissions. You must first create a set before you can use it here. See "Adding System Sets" on page 536 to create a system set. Permissions for these sets must be specified before running the discovery job.
Add systems without known credentials to set	Specify the system set to which you want to add the discovered systems without known credentials. Sets are logical groupings of items (systems, databases, etc.) that allow you to specify additional access to the discovered systems and accounts. For example, you can further grant access to discovered systems using the set-level permissions. You must first create a set before you can use it here. See "Adding System Sets" on page 536 to create a system set. Permissions for these sets must be specified before running the discovery job.
Add discovered accounts to set	Specify the account set to which you want to add the discovered accounts. Sets are logical groupings of items (systems, databases, etc.) that allow you to specify additional access to the discovered systems and accounts. For example, you can further grant access to discovered systems using the set-level permissions. You must first create a set before you can use it here. See "Adding Account Sets" on page 475 to create an account set. Permissions for these sets must be specified before running the discovery job.
Add discovered services to set	Specify the service set to which you want to add the discovered services. Sets are logical groupings of items (systems, databases, etc.) that allow you to specify additional access to the discovered systems and accounts. For example, you can further grant access to discovered systems using the set-level permissions. You must first create a set before you can use it here. See "Adding Service Sets" on page 506 to create a service set. Permissions for these sets must be specified before running the discovery job.

11.

12. Select the option to **Apply Actions to** the specified actions to newly discovered systems only or both new and existing systems.
13. Click **Save**.

Understanding Job Reports

The job report provides a detailed report of the discovered systems. You can click **Download** to save the report.

Understanding Job Summaries

The job summary table provides details about the discovered system.

Updating Passwords for Added Accounts

After you run discovery jobs to add services that run under local or domain accounts to the Privileged Access Service, you might have one or more new unmanaged accounts that have been added to the service but are missing a password.

To check for and add missing passwords:

1. Click the **Resources** > **Accounts**.
2. Select **Local Accounts** from the Sets menu to check for newly-added local accounts that are used to run services.

   If any accounts display the status Missing Password, continue to the next step to add the password for the account to the Privileged Access Service.
3. Select the account, click the Actions menu, then select **Update Password**.
4. Type the password for the account, then click **Save**.
5. Click **Domain Accounts** to check for newly-added domain accounts that are used to run services.

   If any accounts display the status Missing Password, repeat Step 3 and Step 4 to add the password for the account to the Privileged Access Service.
6. Click **Manage this credential** if you want to have the account password for the service account you just updated to be managed by the Privileged Access Service.

Updating Service Settings

After you run discovery jobs to add services that run under local or domain accounts, you need to perform a few additional steps to enable automated password management for each service. Keep in mind that the **service account** is the account that runs an application service or scheduled task. Automated password management also requires an **administrative account**. The administrative account is the account that rotates the service account password.

To prepare for automated password rotation of service account passwords, you need to:

- Identify a stored administrative account that will be used to manage the password for service account. The account must be a domain account stored in the Privileged Access Service and must have the Rotate permission. For more information about granting permission to an account, see "Setting System-Specific Permissions" on page 560. For an overview of what different permissions allow users to so, see "Assigning Profile Management Permissions to Systems" on page 593
- Determine whether you need to create a special account–called a multiplexed account–to ensure password synchronization if a service account runs on multiple computers. For more information about multiplexed accounts, see "Adding Multiplexed Accounts" on page 508
- Set the global- or system-specific password rotation policy on the systems where the service runs. For more information about setting the password rotation policy, see "Enabling Secret Workflow" on page 503
- Update the service settings to enable automated password management.

To update service settings:

1. Click **Resources**, then **Services**, then select a service.
2. Click **Select** to search for and select a domain account.
   - Type a search string to locate the appropriate account.
   - Select the account in the list of results, then click **Add**.
3. Type an optional description for the service.
4. Verify the service type and name.
5. Leave **Enable management of this application password** unselected to continue using the discovered service account.

   You can select **Enable management of this application password** if you want the password for the service account to be managed by the Privileged Access Service. However, this option requires you to create a multiplexed account to replace the service account that was discovered.

   Because additional steps are required to replace the discovered service account, you should not select **Enable management of this application password** unless you have prepared accounts as described in "Adding multiplexed accounts." You can create and configure multiplexed accounts before or after updating the other service settings.

   The remaining fields are only applicable after you select **Enable management of this application password** to automate password rotation. For more information about configuring automatic password rotation, see "Automating Password Rotation" on page 507
6. Click **Save** to save the service settings.

If a service is running under its account when it is time to rotate the password, password rotation is skipped until the service session ends.

Viewing Discovered Services

You can view the global list of discovered and manually added services from the Services tab in the Admin Portal. You can also view the list of discovered services or manually added service information for specific systems. Both the global and system-specific service list provide the following information:

- Name indicates the program name used to run the Windows service or the full path to the scheduled task.
- Description displays the display name associated with the Windows service or scheduled task.
- System indicates the target system where the service runs.
- Multiplexed account is empty until you configure password management for the service. For example, this field is blank for newly discovered services if they run under an account that doesn't have a managed password stored in the Privileged Access Service.
- Current account displays the local or domain account that the service is currently configured to run as.
- Type indicates whether the service is a Windows service or a scheduled task.
- Managed indicates if the service is being managed by Privileged Access Service.
- Issues displays additional information about the status of the service. For example, if the password for the service account is due for rotation but is currently in use on another target system, a message indicating the status is displayed.

- Discovered indicates whether the service was discovered manually or automatically. If it was added to Privileged Access Service via discovery, then this field is left empty.

Viewing Discovered System Information

After a successful discovery job is complete, the new systems, domains, computers, accounts, and services are listed under the appropriate tabs within the Admin Portal. Additionally, you can see the full discovery report from the Discovery History page.

To access the discovery job report:

1. Click **Discovery** > **Systems and Accounts** > **History**.
2. Click the **Show Job History** link associated with the relevant discovery profile.
3. The Job Report window opens in a new tab.
4. You can review the report directly or download it.

Identifying What to Manage

Before adding any objects to the Privileged Access Service, you might want to consider the following:

- Which accounts and account types—local, domain, database, and service—do you want to add to the service?
- Which account passwords should only be managed by the service?
- Are there any restrictions on the accounts you plan to add to the service?

You can store and manage accounts and passwords for different types of network systems, such as servers, workstations, switches, and routers. You can also store and manage passwords for accounts used to access to domains, databases, Windows services, and Windows scheduled tasks.

To get started, you might want to identify which accounts you want to store to support remote access and which accounts have passwords that should be managed. Some of the common local accounts that are likely candidates for being managed through Privileged Access Service include:

- `root`
- `oracle` for Oracle database administration
- `sidadm` for SAP administration
- `db2inst` for IBM DB2 instance administration
- `patrol` for BMC Patrol administration

You might have many other administrative tools or in-house accounts that require special privileges, have access to sensitive information, are used to perform database operations, or are required to run specific services. You can use Privileged Access Services to manage the password for any of these accounts. You can also add any other accounts to securely store the account information without having the password managed.

Importing Systems, Accounts, Domains, and Databases

You can create an import file to add multiple entities (Systems, Accounts, Domains, and Databases) to Privileged Access Service, and their attributes using the import file template and the Delinea PowerShell script. The import file provides a comma-separated set of required and optional fields that describe the items you want to add. Once you

populate the CSV file with the information you want imported into Privileged Access Service, you can run the Delinea PowerShell script and then access the content in the Admin Portal.

To download the import files and populate the CSV file:

1. Access Github at https://github.com/centrify/centrify-samples-powershell to download the import files to your local computer. The import files include the following:
   - Privileged Access Service PowerShell script (Centrify.Samples.PowerShell.Example.ps1)
- You modify the script file to import entities and their attributes from the CSV file into Privileged Access Service.
  - Privileged Access Service PowerShell module file (Centrify.Sample.PowerShell.CPS.psm1)
- The module file is called from the Delinea PowerShell script and does not require any modification.
  - CSV template (Sample.csv)
- The import template illustrates the format to use in creating your own comma-separated values (CSV) file with all the entities and attributes you want to import.

2. Open the Sample.csv template in a text editor or spreadsheet program.
3. Click File, then Save As to save the file to a location on your local computer.
4. Edit your custom CSV file, using the template as a guideline, so that each line provides the information regarding Systems, Domains, Databases, and Accounts you want added to Privileged Access Service.

- As illustrated by the examples in the template file, you can leave optional fields blank. When you are finished adding the entities you want to import, remove the template fields and examples—if you haven't done so already—and save your changes to the file.

For information on the available attributes and what they mean, see "Sample.csv template fields."

To import multiple systems, accounts, domains, and databases:

Verify that the computer you are using to import entities has access to the Privileged Access Service Admin Portal.

1. Open the Centrify.Samples.PowerShell.Example.ps1 script file you downloaded earlier and edit the param section of the script to include the following parameters for your instance:

- #[string]$username = "userexample@acme.com",
- #[string]$endpoint = "https://cloud.centrify.com",

2. Edit the Centrify.Samples.PowerShell.Example.ps1 to include a command like the following, where Endpointincludes your Privileged Access Service tenant and CSVFileincludes the path and name of the CSV file you created. For example:

- Centrify-CPS-Import -Endpoint 'https://cloud.centrify.com' -Token $token -CSVFile 'C:\ImportFile.csv'

3. Save the modified file and then start Windows PowerShell to open a command window.
4. Run the modified Centrify.Samples.PowerShell.Example.ps1 script by entering the full path to the script. For example, C:/scripts/Centrify.Samples.PowerShell.Example.ps1.

- The script calls theDelinea.Sample.PowerShell.CPS.psm1 module to import Systems, Domains, Databases, Accounts and their attributes into Privileged Access Service.
- Depending on the number of entities you are importing, the process might take some time to complete. Once complete, the script outputs the following files to a folder with information on the import status:
  - FailedRows.csv–this file includes all rows that failed to import into Privileged Access Service. You can fix the errors in this file and then re-import the content. If this file is not included in the output, the import was successful.
  - FailedRows.txt–this file provides a summary of the import result for failed rows.
  - WarningRows.txt–this file provides import results for the rows in the CSV file that imported with some errors and an explanation for the errors. If this file is empty, all content in the CSV file imported successfully. If the import fails to complete a particular operation, you can log in to the Admin Portal and correct the failed operation.
  - AllRows.txt–this file provides the results for all rows in the CSV file. The rows in this file are listed in the same order as the Sample.csv.

Sample.csv template fields

The following table describes the template fields in the Sample.csv file. Enter values for each entity type according to the headings designated in the template file. Do not change the template headings; the import functionality requires that the headings match those in the template exactly. The order that you enter entities (Systems, Domains, Databases, and Accounts) into the import file does not affect import functionality.

For this template field	You need to do this
Entity Type	Enter one of the following entity types:SystemDomainDatabaseAccountThis field is required.
Name	Type the display name of the system, domain or database you want to add.As illustrated by the examples in the template, you can have multiple lines with the same name. For example, if you are adding more than one account for the same system, list each account as a separate line with the same system name. This field is required and applies to Systems, Domains, and Databases.
FQDN	Type the fully-qualified domain name or IP address of the System or Database you want to add. If you are only adding an account for a system that was previously added, you should not specify the FQDN field.This field is required and applies to Systems and Databases.
Description	Type any descriptive information you want to add for the entity. This field is optional and applies to Systems, Domains, Databases, and Accounts.

For this template field	You need to do this
ComputerClass	Specify the type of system you are adding. You can specify one of the following values for this field:`WindowsUnixGenericSshCisco AsyncOSCiscoIOSCiscoNXOSJuniperJunosHPNonStopOSIBMiCheckPointGaiaPalo AltoNetworksPANOSF5NetworksBIGIPVMwareVMkernel`This field is required and applies to Systems.
ProxyUser	Type the name of the “proxy” user for a system. This field is optional and applies to Systems. For more information about the “proxy” user for Windows systems, see the following topic:"Configuring Proxy Users for Password Operations" on page 546 For more information about the “proxy” user for UNIX and Juniper systems, see the following topic:"Specifying Proxy Root Accounts" on page 537
ProxyUserPassword	Provide the password for the “proxy” user for a system. This field is optional and applies to Systems.
ProxyUserIsManaged	Specify whether you want to manage the password for the “proxy” user. This field is optional and applies to Systems. You can specify TRUE if you want the Privileged Access Service to manage the password for the “proxy” account, or FALSE if you want to leave the password unmanaged.
ResourceDomain	Type the name of the domain that the system is joined to. This field is optional and applies to Systems.
ResourceDomainOperationsEnabled	Specify whether you want to use the domain administrative account to enable zone role workflow. You specify TRUE if you want to use the domain administrative account to enable operations such as zone role workflow, or FALSE if you do not want to use the domain administrative account to enable domain operations. In order to enable domain operations for a system, the user must have grant rights over the domain or else the import will fail. This field is optional and applies to Systems.
ResourceSessionType	Specify whether you want to use secure shell or remote desktop for remote connections. Enter Ssh for secure shell or Rdp for remote desktop. This field is required and applies to Systems.
ResourceSessionTypePort	Enter the port to be used for remote connections. You only need to enter a value if you do not want to use the default port (default port for SSH is 22 and for RDP it is 3389). This field is optional and applies to Systems.
ResourceWindowsManagementMode	For Windows System types , you can choose a management mode to manage the system.Enter one of the following management modes:Unknown (this is equivalent to auto-detect in the Admin Portal)SmbWinRMOverHttpWinRMOverHttpsRpcOverTcpDisabledThis field is optional and applies to Systems.

For this template field	You need to do this
ResourceWindowsManagementPort	For Windows, F5 Networks BIG-IP, and Palo Alto Networks PAN-OS Systems, enter the management port to be used for password management. This field is optional and applies to Systems.
PasswordProfile	Enter a name to add a customized password profile to define the rules applied when managed passwords are generated for systems, domains, or databases. For more information about customizing a password profile, see "Configuring password profiles."This field is optional and applies to Systems, Domains, and Databases.
SetName	Enter a name for system, domain, database, or account sets. Sets are logical groups of a particular type (system, domain, database, or account) to simplify management activity and reporting for entities with attributes in common. To enter more than one set name for an entity, separate the entries by a |. For example, SystemSet1|SystemSet2|SystemSet3.This field is optional and applies to Systems, Domains, Databases, and Accounts.
DefaultCheckoutTime	Enter a number to specify the length of time (in minutes) that a checked out password is valid. The minimum checkout time is 15 minutes. If no value is specified, the default is 60 minutes. Also see Setting system-specific policies. This field is optional and applies to Systems, Domains, Databases, and Accounts.
AllowRemote	Enter TRUE if you want to allow remote connections from a public network for a selected system of FALSE if you do not want to allow remote connections from a public network.This field is optional and applies to Systems.
ParentEntityTypeOfAccount	Enter the type of entity related to the account (System, Domain or Database).This field is required and applies to Accounts.
ParentEntityNameOfAccount	Enter the display name of the system, domain or database associated with the account. This field is required and applies to Accounts.
User	Type the user name for an account to be used with Systems, Domains, and Databases. This field is required and applies to Accounts.
Password	Type the password for the account to be used with the system.This field is optional and applies to Accounts.
IsManaged	Specify whether you want to manage the password for the user account you are adding for the system.You can specify TRUE if you want the Privileged Access Service to manage the password for the account, or FALSE if you want to leave the password unmanaged.This field is optional and applies to Accounts.
AccountMode	Enter the term Expert to add an expert mode account for Checkpoint Gaia systems. This field is optional and applies to Systems.

For this template field	You need to do this
UseProxy	Specify whether you want to add a “proxy” account for the system.Specify TRUE if you want to use a “proxy” account, or FALSE if you don’t want to add a “proxy” account for the system.For UNIX and Juniper systems, use this field if your secure shell environment is configured to not allow the root user to access computers remotely using SSH. You can also use this field for Windows systems if you want to use a proxy account for Windows Remote Management (WinRM) connections to a system.This field is optional and applies to Accounts.
DatabaseServiceType	Specify the type of database you are adding.Enter one of the following types:SQLServerOracleSAP Adaptive Server Enterprise (ASE)This field is required and applies to Databases.
OracleServiceName	For Oracle databases, you must enter the service name assigned to the Oracle database. Also see "Adding Databases" on page 477. This field is required and applies to Databases.
SQLInstanceName	For SQL Server databases, you must enter the instance name assigned to the database. Also see "Adding Databases" on page 477. This field is optional and applies to Databases.
DatabasePort	Specify the port number used to check the status of the database and when updating database passwords. This field is optional and applies to Databases.
ParentDomain	If a child domain is configured, enter the name of its parent domain.This field is optional and applies to Domains.
AdministrativeAccount	Enter an account in the format admin@childdomain, admin@mycompany.com or a local account that needs to be set as the administrative account.This field is optional and applies to Systems and Domains.
AllowAutomaticAccountMaintenance	Specify TRUE to allow out-of-sync passwords to be reset and managed accounts to be unlocked during login or checkout, or FALSE if you do not want to allow it. Requires an Administrative Account be defined for the domain.This field is optional and applies to Domains.
AllowManualAccountUnlock	Specify TRUE to allow users with the Unlock Account permission to manually unlock accounts, or FALSE if you do not want to allow accounts to be manually unlocked. Requires an Administrative Account be defined for the domain.This field is optional and applies to Domains.

For this template field	You need to do this
AllowMultipleCheckouts	Specify whether multiple users can have the same domain account password checked out at the same time for a system, domain, or database.Enter FALSE if only one user is allowed to check out the password at any given time. Enter TRUE if you want to allow multiple users to have the account password checked out at the same time without waiting for the password to be checked in. Also see, Allow multiple password checkouts. This field is optional and applies to Systems, Domains, and Databases.
AllowPasswordRotation	Specifies if the managed password should be rotated periodically by Privileged Access Service for a system, domain, or database.Enter TRUE to allow periodic password rotation or FALSE to not allow periodic password rotation.This field is optional and applies to Systems, Domains, and Databases.
PasswordRotateDuration	Specifies the interval at which managed passwords are automatically rotated.Enter the maximum number of days to allow between automated password changes for managed system, domain, or database accounts.This field is optional and applies to Systems, Domains, and Databases.
MinimumPasswordAge	Enter the minimum number of days before a password must be rotated.This field is optional and applies to Systems, Domains, and Databases.
AllowPasswordHistoryCleanUp	Specifies if the retired passwords should be deleted periodically by Privileged Access Service.Enter TRUE to allow periodic password history cleanupor FALSE to not allow periodic password history cleanup.This field is optional and applies to Systems, Domains, and Databases.
PasswordHistoryCleanUpDuration	Enter the number of days after which retired passwords matching the duration are deleted.This field is optional and applies to Systems, Domains, and Databases.

Importing Systems and Accounts

If you are familiar with the information required to add systems and shared accounts, you can create an import file to add multiple systems and shared accounts at once. The import file provides a comma-separated set of required and optional fields that describe the systems and accounts you want to add.

To import additional entities, see "Importing Systems, Accounts, Domains, and Databases" on page 1189

To import multiple systems and accounts:

1. In the Admin Portal, click **Resources** then click **Systems** to display the list of computers and network devices.
2. Click **Import**.
3. Click **Bulk System Import Template** to download the template for importing systems and, optionally, accounts.

The import template illustrates the format to use in creating your own comma-separated values (CSV) file with the systems and accounts you want to import. The template also provides an example of how you might add two accounts for the system named host2.

4. Open the import template in a text editor or spreadsheet program.
5. Click **File**, then **Save As** to save the file in a location you can browse to from the Admin Portal.
6. Edit your custom file so that each line provides the following information for a specific system:

For this template field	You need to do this
Name	Type the display name of the system you want to add. This field is required. As illustrated by the example in the template, you can have multiple lines with the same system name. For example, if you are adding more than one account for the same system, list each account as a separate line with the same system name.
FQDN	Type the fully-qualified domain name or IP address of the system you want to add. This field is required if a row adds both a system and an account or if the row adds a system. If you are only adding an account for a system that was previously added, you should not specify the FQDN field.

For this template field	You need to do this
ComputerClass	Specify the type of system you are adding. You can specify one of the following for the **ComputerClass** field: - Windows - Unix - GenericSsh - CiscoIOS - CiscoNXOS - CiscoAsyncOS - CustomSsh >**Note:** The CustomSsh ComputerClass system type is for adding a system with a custom resource profile. For these custom system types, you must also specify the CustomIdentifier field. - JuniperJunos - HPNonStopOS - IBMi - CheckPointGaia - VMwareVMkernel To import Palo Alto Networks PAN-OS or F5 Networks BIG-IP systems, see "Importing Systems and Accounts" on page 621
Description	Type any descriptive information you want to add for the system. This field is optional.
ProxyUserPassword	Provide the password for the “proxy” user for a system. This field is optional. For more information about the “proxy” user for Windows systems, see the following topic: "Configuring Proxy Users for Password Operations" on page 546 For more information about the “proxy” user for UNIX and Juniper systems, see the following topic: "Specifying Proxy Root Accounts" on page 537

For this template field	You need to do this
ProxyUser	Type the name of the “proxy” user for a system. This field is optional. For more information about the “proxy” user for Windows systems, see: "Configuring Proxy Users for Password Operations" on page 546 For more information about the “proxy” user for UNIX and Juniper systems, see: "Specifying Proxy Root Accounts" on page 537
ProxyUserIsManaged	Specify whether you want to manage the password for the “proxy” user. This field is optional. You can specify TRUE if you want the Privileged Access Service to manage the password for the “proxy” account, or FALSE if you want to leave the password unmanaged.
User	Type the user name for an account to be used with the system. This field is optional.
Password	Type the password for the account to be used with the system. This field is optional.
Managed	Specify whether you want to manage the password for the user account you are adding for the system. This field is optional. You can specify TRUE if you want the Privileged Access Service to manage the password for the account, or FALSE if you want to leave the password unmanaged.
UseProxy	Specify whether you want to add a “proxy” account for the system. This field is optional. You can specify TRUE if you want to use a “proxy” account, or FALSE if you don’t want to add a “proxy” account for the system. For UNIX and Juniper systems, use this field if your secure shell environment is configured to not allow the root user to access computers remotely using SSH. You can also use this field for Windows systems if you want to use a proxy account for Windows Remote Management (WinRM) connections to a system.
UserDescription	Type any descriptive information you want to add for the user account. This field is optional.

For this template field	You need to do this
Domain	Type the name of the domain that the system is joined to. This field is optional.
DomainOperationsEnabled	Specify whether you want to use the domain administrative account to enable zone role workflow. This field is optional. You specify TRUE if you want to use the domain administrative account to enable operations such as zone role workflow, or FALSE if you do not want to use the domain administrative account to enable domain operations. In order to enable domain operations for a system, the user must have grant rights over the domain or else the import will fail.
PasswordProfiles	Enter a name to add a customized password profile to define the rules applied when managed passwords are generated for a system. This field is optional. For more information about customizing a password profile, see "Configuring Password Profiles" on page 751
CustomIdentifer	Specify the resource profile identifier for custom system types. **Note:** the ComputerClass must be specified as "CustomSsh" for custom system types.

As illustrated by the examples in the template file, you can leave optional fields blank. When you are finished adding the systems and accounts you want to import, remove the template fields and examples–if you haven't done so already–and save your changes to the file.

1. In the Admin Portal, click ***Resources***, then click **Systems** to display the list of computers and network devices.
2. Click **Import**.
3. Click **Browse** to select your customized CSV file, verify the email address for notification of the import result, then click **Import**.

   The import process runs in the background. Depending on the number of systems and accounts you are importing, the process might take some time to complete. You will receive email notification of the results when the import process is complete.

Importing Servers with a Custom Resource Profile

To import a server that uses a custom resource profile, follow the general steps above. In the Bulk System Import Template, use the settings below:

- Set the **ComputerClass** column (Column C) to the value CustomSsh.
- Set the **CustomIdentifier** column (Column P) to the name of your custom resource profile.

Adding and Managing Resource Profiles

When adding a system to Delinea Privileged Access Service, you select the *type* of the target system. This selection of type tells the Delinea PAS system how to interact with the system to login and manage passwords. Delinea PAS supports a number of built-in system types. You expand this support by adding additional *custom*

types (for example: to support a router that does not have built-in support). Select the System Type from the drop-down. You may filter the system types drop-down to display only Built-in or only Custom types by using the checkboxes next to the drop-down.

To add a custom system type, you add a *Resource Profile* that includes a script detailing how Delinea PAS should interact with the device. The target system type must support the SSH protocol for logging into the system and managing passwords.

To add and manage resource profiles, perform the following steps in this order:

1. "Writing a custom script"
2. "Creating and managing a resource profile"
3. "Importing and exporting resource profile packages"
4. "Adding a system from a resource profile"
5. "Script functions, arguments, and exit codes for resource profiles"

Adding Systems from Resource Profiles

Now that you have a new system type, you can navigate to **Resources** > **Systems** and when you click **Add System** you can choose the system type you just created.

Note: You can filter system types to show custom types only by clicking **Custom**.

Once you add the system, you can then add accounts, configure settings, and perform operations like normal. All operations going through the account are managed through the script that you created.

Operations that you can perform may include:

- Login
- Checkout
- Update Password
- Rotate Password
- Add to Set
- Verify Credential
- Delete
- Password Reconciliation

Script Functions, Arguments, and Exit Codes for Resource Profiles

The following are resource profile script functions, arguments and exit codes.

Script Functions for Resource Profiles

The following are script functions for Resource Profile scripts.

User-Supplied Script Functions

Script function	Description
getAttributes	function getAttributes()
verifyPassword	function verifyPassword(verifyPasswordInfo)
changePassword	function changePassword(changePasswordInfo)
setPassword	function setPassword(setPasswordInfo)
switchUser	function switchUser(switchUserInfo)

System-Supplied Script Functions

Script function	Description
sshSend	sshSend(data)
sshExpect	sshExpect(regularExpressions)
sshWaitForNoOutput	sshWaitForNoOutput(waitMilliseconds)
stringify	stringify(object)
verbose	verbose(text)
info	info(text)
warn	warn(text)
error	error(text)

Script Function Return Values

- Success
- ErrorFailed
- ErrorInvalidUserPassword
- ErrorInvalidAdminPassword
- ErrorUnexpectedResult
- ErrorUncertainResult

SshTest Command Arguments for Resource Profiles

SshTest.exe [Options]

Command	Description
-h, --help	Displays usage.
-s, --script	File name of the script.
-l, --load	Load and verify script.
-v, --verify	Verify user password.
-c, --change	Change user password.
-r, --reset	Reset user's password.
-w, --switch	Switch user account.
-h, --host	FQDN of the target system.
-u, --user	Username.
-p, --password	Password.
-n, --new-password	New password.
-m, --management-user	Management user.
-a, --management-password	Management user's password.
-x, --proxy	Proxy user name.
-y, --proxy-password	Proxy password.
--port	(Default: 22) SSH TCP port.
--log-level	(Default: Verbose) Logging level (Verbose, Info,Warn, or Error).
--show-connection-log	(Default: False) Display SSH connection logging messages.
--show-detailed-log	(Default: False) Display 'expect' and other internal logging messages.
--show-passwords	(Default: False) Display passwords in logging messages.
--version	Display version.
--help	Display this help screen.

SshTest Exit Codes

The SSH test utility returns an exit code upon completion. This exit code can be used in test script to automate testing of your scripts. The values are as follows:

Exit code values	Description
0	Success.
1	ErrorFailed.
2	ErrorInvalidUserPassword.
3	ErrorInvalidAdminPassword.
4	ErrorInvalidProxyPassword.
5	ErrorUnexpectedResult.
6	ErrorUncertainResult.
7	ErrorChangePasswordNotSupported.
8	ErrorSetPasswordNotSupported.
9	ErrorProxyAccountNotSupported.

Importing and Exporting Resource Profiles

To share resource profiles among tenants, you can export a resource profile to a resource profile package file. This allows for another tenant to then import that resource profile package. Resource profiles may be imported and exported as resource packages. The package is a zip file containing the following:

- manifest.json – manifest file with meta-data.
- script.js.
- icon.png (optional).
- password-profile.json – password profile (optional).

There are no directory structures in the zip. The text files in resource profile packages (scripts, manifest, and password profile) are in UTF-8 encoding. Line endings may be either CRLF or LF.

Note: Other file names are permitted but must start with the names given above. For example: manifest-PAN311.json.

The documentation below provides steps to perform the following:

- Importing Resource Profile Packages
- Exporting Resource Profile Packages
- Updating Existing Resource Profiles from a Resource Profile Package
- Manually Creating and Modifying Resource Profile Packages
- Using Sets with Resource Profiles

Importing Resource Profile Packages

You can import previously exported resource profile packages. Things to keep in mind before you import a profile package:

- If the resource profile package has a password profile, you are given the option to ignore it and specify an existing password profile. You can create a new profile based on the information in the package or manually create a password profile.
- The information in the package is used to initialize a form for creating the new resource profile. You can edit the resource profile before saving it.

To import a resource profile package

1. In the Admin Portal, navigate to Settings > Resources > Resource Profiles > Import Profile. A warning message appears to ensure the package is from a trusted source.
2. Click Continue and proceed to import profile package. Click Browse to add your package and assign Password Complexity Profile to custom or package settings:
3. The details of the imported package will appear. Confirm all the fields to the package are correct or amend as needed. Click Save.

Exporting Resource Profile Packages

You can export a resource profile package from an existing resource profile. The .zip contains the following:

- manifest-.json.
- script-.js.
- icon-.png.
- password-profile-.json.

Note: There is no directory structure. When exporting, you can export the optional icon and password profile components of the package.

To export a resource profile package

1. In the Admin Portal, navigate to Settings > Resources > Resource Profiles. Choose a profile and navigate to Actions and choose Export.
2. An Export Profile window appears. Name the package and check off if you want to include the Password Profile and Logo.
3. Click Export and you will see the downloaded package in your Downloads folder.

Updating Existing Resource Profiles from a Resource Profile Package

After you have imported a resource profile package, at a later date you might want to update it with the "latest copy" of the resource profile (for example, the script may have been updated).

To update a resource profile package

1. In the Admin Portal, navigate to Settings > Resources > Resource Profiles. Choose a profile to update. Navigate to Actions and choose Update.

- Here, you can update the:
  - Script.
  - Manifest.
  - Icon.
  - Password Profile.

2. Make changes as needed and click Update. The profile package will appear. Confirm all the components are correct and click Save.

Manually Creating and Modifying Resource Profile Packages

You can manually create and modify resource profile packages. To create a resource package manually:

1. Write a script and create a manifest file (using the editor of your choice).
2. Create an icon (optional).
3. Create Resource Profile Package password profile file.
4. Create a zip with these files. The zip is a resource profile package that can be imported.

Resource Profile Package Manifest

The manifest file is JSON as in the following example:

```
{
"Identifier": "Pan311",
"Name": "PAN 311",
"Description": "{ \"en\": \"PAN 311 Description\", \"es\": \"Descripcion de PAN 311\" }",
"Author": "Rich Smith",
"Version": "4.4.4.4"
}
```

Resource Profile Package Password Profile

The optional password profile allows a package developer to suggest the settings for a password profile that works for the device (example: has particular device requirements for password generation).

Note: When importing a package, you can ignore the password profile in the package in favor of your own password profile.

The password profile is JSON as in the following example:

```
{
"Name": "dev2 profile",
"Description": "dev2 password profile",
"MinimumPasswordLength": 6,
"MaximumPasswordLength": 8,
"AtLeastOneLowercase": true,
```

"AtLeastOneUppercase": true,
"AtLeastOneDigit": true,
"ConsecutiveCharRepeatAllowed": true,
"AtLeastOneSpecial": true,
"MaximumCharOccurrenceCount": 2,
"SpecialCharSet": "!$%&()*+,-./:;<=>?[\\]^_{|}~",
"FirstCharacterType": "AnyChar",
"LastCharacterType:" "AnyChar",
"MinimumAlphabeticCharacterCount": 2,
"MinimumNonAlphabeticCharacterCount": 2
}

Using Sets with Resource Profiles

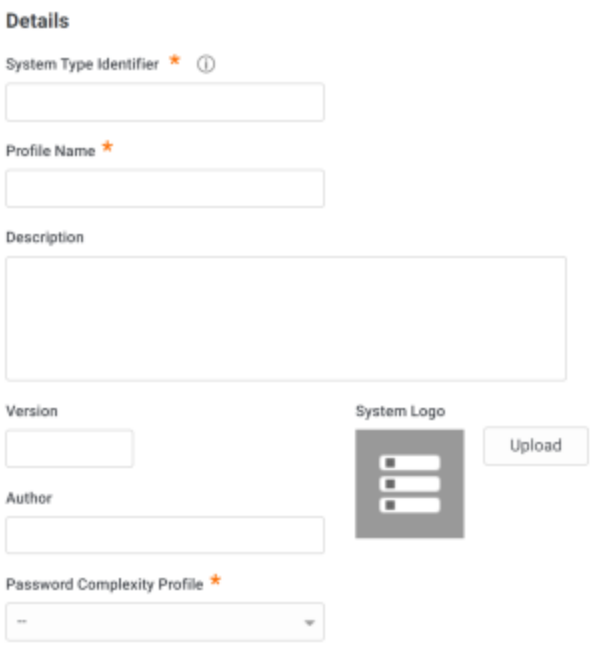
You can add sets to resource profiles. For more information on managing sets, see "Managing Sets" on page 684.

Creating and Managing Resource Profiles

Adding Resource Profiles

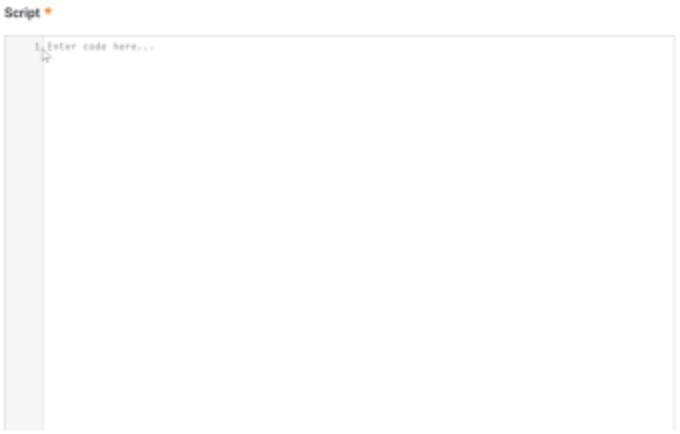
Note: You must have Privileged Access Service Administrator or System Administrator rights to create a custom resource.

1. In the Admin Portal, navigate to **Settings** > **Resources** > **ResourceProfiles** and choose **Add Profile**. For the first part of the add profile, enter fields as seen below:

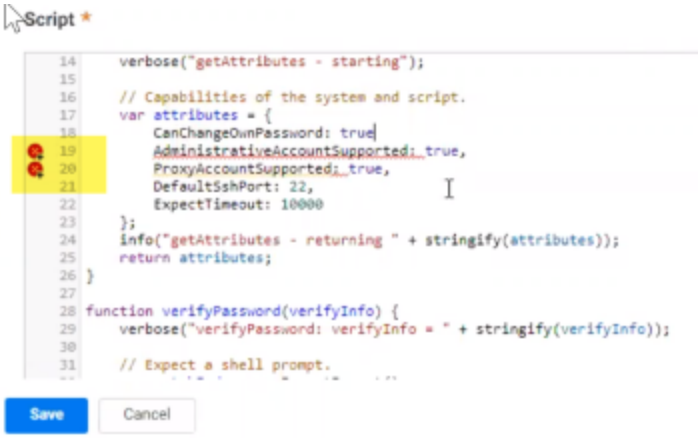


The required fields are as follows:

- **System Type Identifier***: The system type shown in the **Add System** wizard.
- **Profile Name***: a display name for the system.
- **Description**: system description.
- **Version**: assign version to system.
- **SystemLogo**: upload a logo for your system.
- **Author**: system author.
- **Password Complexity Profile***: allows you to choose an existing profile or create your own. To create your own profile, choose **Add New Profile**, see "Configuring password profiles."
- **Script***: Enter a resource profile script. You may copy and paste your script into this field:



If there are any syntax errors in the script, you will see a red flag as shown below:



Updating Resource Profile Settings

To update resource profile settings, navigate to **Settings** > **Resources** > **ResourceProfiles** and choose an existing profile where you can edit the profile fields.

"Adding or updating resource profile permissions"

Add a user, group, or role to grant permissions to this resource profile.

"Resource profile activity"

View resource profile activity by date and detail.

Writing Custom Scripts

The following describes how to write a custom system script used to create a resource profile. Once the system script is written, you may add or update a resource profile that contains the script and then add a system of that type.

Note: Scripts must be written in JavaScript, extensive JavaScript knowledge is not required.

The script must implement two functions as follows:

Functions

getAttributes()

The script must implement the getAttributes() function. It indicates the functionality your script provides and additional configuration information.

Example:

```
function getAttributes() {
var attributes = {
CanChangeOwnPassword: false,
AdministrativeAccountSupported: false
};
return attributes;
}
```

The remaining functions you write consist of *send* and *expect* verbs that are invoked with the sshSend() and sshExpect() functions.

verifyPassword()

The verifyPassword() function is required and allows Privileged Access Service to determine if a username/password combination is valid. When the verifyPassword() function is invoked, Privileged Access Service logs into the system and nothing more may be needed to validate that the user name and password combination is valid.

Example:

Note: The following is an implementation of verifyPassword() that ensures a command prompt outputs by the target system:

```
function verifyPassword(verifyPasswordInfo) {
// Expect a prompt.
var result = sshExpect(["Prompt> $"]);
if (result.MatchIndex < 0) {
```

```
return ErrorInvalidUserPassword;
}
// Password is OK.
return Success;
}
```

sshExpect()

The following are true for sshExpect():

- The sshExpect() function is called and commands to wait until the target system outputs the string "Prompt> ".
- If the target system does not output the expected string, your script returns an error code.
- The argument to the sshExpect() function is a list of regular expressions to expect.
- If the result.MatchIndex returned is less than zero, the expected string was not output by the target system.

Putting It All Together

Finally, put together the complete script as follows:

```
function getAttributes() {
var attributes = {
CanChangeOwnPassword: false,
AdministrativeAccountSupported: false
};
return attributes;
}
function verifyPassword(verifyPasswordInfo) {
// Expect a prompt.
var result = sshExpect(["Prompt> $"]);
if (result.MatchIndex < 0) {
return ErrorInvalidUserPassword;
}
// Password is OK.
return Success;
}
```

You can now create a new resource profile with this script and start adding systems of this type. This script allows you to create systems and accounts with vaulted passwords, control who has access to those accounts, initiate workflow for requesting temporary access to a system, and audit use of an account.

Testing the Script

A standalone SSH test utility allows you to test and debug your script before using it to create a resource profile. The test utility runs on Windows systems and is a command-line tool suitable for integration into a test harness. To download the SSH test utility, from the Admin Portal, navigate to **Download** > **Tools** > **Centrify SSH Test Kit**.

Test Loading

Take the script you created and add it to a file entitled "device-script.js". You can now add a number of arguments to SSH test utility, many of which are optional. You must, however, specify the --script parameter, and one of the "operation" parameters such as --load.

Example:

```
> SshTest --script device-script.js --load
TEST(Info): Load script result = Success
>
```

The --load parameter asks SSH test utility to load the JavaScript, test for syntax errors, invoke the getAttributes() function and verify that the attributes are legal.

Example:

Modify the script to include a syntax error by removing the colon after CanChangeOwnPassword in the getAttributes() function as follows:

```
function getAttributes() {
var attributes = {
CanChangeOwnPassword false,
AdministrativeAccountSupported: false
};
return attributes;
}
function verifyPassword(verifyPasswordInfo) {

// Expect a prompt.
var result = sshExpect(["Prompt> $"]);
if (result.MatchIndex < 0) {
return ErrorInvalidUserPassword;
}

// Password is OK.
return Success;
}
```

Now, SSH test utility reports the error:

```
> SshTest --script device-script.js --load
TEST(Error): no viable alternative at input 'CanChangeOwnPassword' at line 4:9
>
```

Similarly, put the colon back in and change the attribute to an invalid one:

```
function getAttributes() {
var attributes = {
ThisIsNotAValidAttribute: false,
AdministrativeAccountSupported: false
};
return attributes;
}
function verifyPassword(verifyPasswordInfo) {

// Expect a prompt.
var result = sshExpect(["Prompt> $"]);
if (result.MatchIndex < 0) {
return ErrorInvalidUserPassword;
}

// Password is OK.
return Success;
}
```

SSH test utility reports the error as follows:

```
> SshTest --script device-script.js --load
TEST(Error): Attribute 'ThisIsNotAValidAttribute' is not valid
>
```

Testing Password Verification

To test your verifyPassword() function, use the --verify parameter and supply additional arguments.

Example:

```
> SshTest --script device-script.js --verify --host hatter-rh.richl.devp --user local2 --
password local2pass
TEST(Info): Verify password result = Success
>
```

Using Script Parameter Shortcuts

Many SSH test utility parameters have shortcuts for the parameter names.

Example, instead of:

```
> SshTest --script device-script.js --verify --host hatter-rh.richl.devp --user local2 --
password local2pass
```

use:

```
> SshTest -s device-script.js -v -h hatter-rh.richl.devp -u local2 -p local2pass
```

Using Script Logging

You can get additional logging output to help diagnose issues with your scripts. For example, to see details of the "send/expect" interaction with the target system, use the --show-detailed-log parameter:

Example:

```
> SshTest -s device-script.js -v -h hatter-rh.richl.devp -u local2 -p local2pass --show-
detailed-log
INTE(Verbose): getAttributes() completed using 3 statements (start=4, end=7)
INTE(Verbose): sshExpect: expect=(Count=1, Values=('Prompt> $'))
INTE(Verbose): Matching: 'Prompt> $' to '^[]0;local2@hatter-rh:~^GPrompt> '
INTE(Verbose): Matched: 'Prompt> $' to 'Prompt> '
INTE(Verbose): sshExpect: found 'Prompt> $' with match index 0
INTE(Verbose): verifyPassword() completed using 4 statements (start=7, end=11)
TEST(Info): Verify password result = Success
>
```

- Messages with an INTE prefix indicate messages generated internally by the script processor.
- Messages with a TEST prefix come directly from the SSH test utility.

Additional Logging

You can add additional logging into your script to help diagnose problems. For example change your script as follows:

```
function getAttributes() {
var attributes = {
CanChangeOwnPassword false,
AdministrativeAccountSupported: false
};
return attributes;
}
function verifyPassword(verifyPasswordInfo) {
verbose("Starting execution of verifyPassword");
verbose("userName = " + verifyPasswordInfo.userName);
verbose("userPassword = " + verifyPasswordInfo.userPassword);

// Expect a prompt.
var result = sshExpect(["Prompt> $"]);
if (result.MatchIndex < 0) {
return ErrorInvalidUserPassword;
}
verbose("Everything went OK");

// Password is OK.
```

```
return Success;
}
```

Messages that you generate from your script have a JINT prefix to indicate they came from the JavaScript interpreter:

```
> SshTest -s device-script.js -v -h hatter-rh.richl.devp -u local2 -p local2pass --show-
detailed-log
JINT(Verbose): Starting execution of verifyPassword
JINT(Verbose): userName = local2
JINT(Verbose): userPassword = <hidden>
JINT(Verbose): Everything went OK
TEST(Info): Verify password result = Success
>
```

View Password Parameter

For security, the password is scrubbed from the output of the SSH test utility. To view the password passed to your verifyPassword() method, use the --show-passwords option.

```
> SshTest -s device-script.js -v -h hatter-rh.richl.devp -u local2 -p local2pass --show-
detailed-log --show-passwords
JINT(Verbose): Starting execution of verifyPassword
JINT(Verbose): userName = local2
JINT(Verbose): userPassword = local2pass
JINT(Verbose): Everything went OK
TEST(Info): Verify password result = Success
>
```

Note: If you are verifying a username and password and see that your verifyPassword() function is not called, there may be a connection issue.

In the following example, where the target system is not running, you might see:

```
> SshTest -s device-script.js -v -h hatter-rh.richl.devp -u local2 -p local2pass
TEST(Error): Connection failed: A connection attempt failed because the connected party
did not properly respond after a period of time, or established connection failed because
connected host has failed to respond 172.27.14.237:22
```

Connection Details Parameter

In the unlikely event there is an error in establishing the connection, you can use the --show-connection-log parameter to see all the details of connection establishment.

Preparing to Deploy Resources

If you are planning to deploy resources to manage privileged account passwords and privilege elevation, you might want to take the following steps before you add any accounts, computers, or network devices:

- Identify What to Manage
- Review the Firewall Rules
- Automatically Discover Servers and Workstations
- You can also add multiple entities (Systems, Accounts, Domains, and Databases) and their attributes using an import file template.

Setting Access Challenge Policies

You can set access challenge policies for individual secrets or folders. For example, you might want to require multi-factor authentication for users who have permission to view, edit, retrieve, or replace secrets if certain conditions are met.

An authentication rule specifies the conditions to be evaluated and the authentication profile specifies the challenges presented when the conditions specified are true. You can configure new authentication rules and authentication profiles just for secrets and folders or select and use rules and profiles you have previously created.

Policy Inheritance

Also note the following behavior for multi-factor authentication inheritance:

- Multi-factor authentication policies are inherited and apply to Retrieve, Move, and Delete actions for folders and secrets.
- Folders and secrets take on authentication policies of the closest parent. For instance, a secret in Production/DevSys will take on the policies of the folder DevSys, not Production, if no polices are applied to the secret.
- Multi-factor authentication policies set for a folder or secret, take precedence over any policy set for a parent folder.

To Set Access Policies for Secrets and Folders:

1. In the Admin Portal, click **Resources**, then click **Secrets** to display the list of secrets or folders.
2. Select the secret or folder to display its details.
   - For Secrets, click the secret to display its details.
   - For Folders, click the check box next to the folder name and then click **Edit** from the Actions menu.
3. Click **Policy**.
4. Select a default access challenge profile, if an appropriate profile exists, or click **Add Rule** to configure one or more authentication challenge rules.
5. Click **Save**.

For more information about how to configure authentication rules and profiles, see "Creating Authentication Rules" on page 281 and "Creating Authentication Profiles" on page 284.

Setting System-Specific Policies

You can set policies for individual systems or set global policies to apply to all systems you add to the Privileged Access Service except where you have explicitly defined a system-specific policy. If you use a combination of global and system-specific policies, the system-specific policies take precedence over the global policies you set.

If you have the appropriate permissions to set global system policies, see "Setting Global Security Options" on page 753 for more information. If you are not using global policies, only want to set policies on individual systems, or want to override global policies on specific systems, you can set the following policies on a case-by-case basis:

- "Allow Remote Access from a Public Network" below
- "Allow RDP Client to Sync Local Clipboard with Remote Session" below
- "Checkout Lifetime" on the next page
- "System Login Challenge Rules and Default Profile" on the next page
- "Authentication if Managing the Service On-Site" on page 643
- "Privilege Elevation Challenge Rules and Default Profile" on page 643
- "Enabling Client Automatic Updates" on page 644

To Set System-Specific Policies:

1. In the Admin Portal, click **Resources**, then click **Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Click **Policy**.
4. Select settings for any or all of the system policies.
5. Click **Save**.

For more information about how to set the system-specific policies, click the policy link or the information icon in the Admin Portal.

Allow Remote Access from a Public Network

Select Yes if you want to allow remote connections from inside or outside of a defined corporate IP address range. If you select Yes, administrators can log on remotely to the selected system from computers or devices that are inside or outside of the corporate IP address range. If you select No, administrators will be denied access if they attempt to log on to the selected system from a connection outside of the corporate IP address range.

If you do not specify a corporate IP address range to define your internal network, all IP addresses are treated as external connections from outside of the firewall and remote access is denied by default.

Allow RDP Client to Sync Local Clipboard with Remote Session

Select Yes for the ability to copy and paste text or images while in a web based RDP session. When enabled, allows you to copy texts or images from a local machine and paste them to the remote session and vice versa. Applies to RDP native client and web clients as follows:

Browser	Text support	Image support
Chrome	Supported	Supported
Edge	Supported	Supported
Internet Explorer 11	Supported	Not supported
Safari	Not supported	Not supported
Firefox	Not supported	Not supported

Checkout Lifetime

Type the maximum number of minutes administrators are allowed to have a password checked out. After the number of minutes specified, the Privileged Access Service automatically checks the password back in. The minimum checkout lifetime is 15 minutes. If the policy is not defined, the default checkout lifetime is 60 minutes.

You can extend the checkout time for a password as long as you do so before the initial checkout period expires. For example, if the maximum checkout lifetime is 60 minutes and you extend the checkout time before the 60 minute period is over, the password expiration is reset to the 60 minute checkout lifetime. For more information about configuring the Checkout lifetime policy, see "Extending Password Checkout Time" on page 464.

System Login Challenge Rules and Default Profile

You can configure authentication rules and authentication profiles to protect remote login access for specific systems. Based on the rules you define, users attempting to log on to a system without knowing the stored account password or using specified credentials might be required to answer a security question, answer a phone call, or click a link in an email message to authentication their identity. The authentication rule defines the conditions for when a specific authentication profile should be used. The authentication profile defines the types of challenges presented and whether one-factor or two-factor authentication is required. You can also define a default authentication profile to use if the conditions you specify for the account login rules are not met.

If you don't create any authentication rules or authentication profiles for logging on without knowing the password for an account, users with the appropriate permission can log on using stored account passwords without being challenged to re-authenticate their identity. If you add authentication rules, a default authentication profile, or both, the policies are evaluated for all attempts to log on to the target system, whether using a stored account password or a specified user name and password.

Supported Authentication Challenges

You should note that only the authentication challenges that are available in a user profile can be presented. For example, you might select **Phone call** and **Email confirmation code** in the authentication profile, but these challenges are only valid if users have both a phone number and email address stored for their accounts.

If users only have a phone number and not an email address stored, they will receive a phone call to complete the authentication process rather than be prompted to select an authentication option. If users have both a phone number and an email address stored, they will be prompted to select which form of authentication to use.

Authentication if Managing the Service On-Site

If you have installed Privileged Access Service on your internal network or in a location where you are managing the service yourself, you can define authentication profiles that use most of the same challenges as when the Privileged Access Service is deployed as a cloud-based service. However, some challenges—such as the Email configuration code and Text message confirmation code—require you to configure settings to support outgoing email and SMS-based text messaging.

You can configure the settings for a custom Simple Mail Transport Protocol (SMTP) mail server and a Twilio in the Admin Portal. To support the Mobile Authenticator as a challenge, you must have a properly registered mobile device. For details about post-installation configuration steps when you deploy Privileged Access Service as an on-site service, see the *Installation and Configuration Guide for OnSite Deployment*.

To Add an Authentication Rule and Profile for Remote Login Access:

1. In the Admin Portal, click **Resources**, then click **Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Click **Policy**.
4. Under System Login Challenge Rules, click **Add Rule**.
5. Click **Add Rule** to define the conditions to evaluate to determine the authentication profile to use when users attempt to log on to a selected system using the stored account password.

   For example, click **Add Rule**, select a condition such as IP Address and inside of the corporate range, then click **Add**. You can add more than one condition to the rule. However, all conditions must be true for the rule to apply.
6. Select the authentication profile to use when all of the conditions you specify are true, then click **OK**.
   - You can select any existing authentication profile if an appropriate profile has been previously-defined in the Admin Portal for the Privileged Access Service.
   - You can select **Not Allowed** as the authentication profile if you want to prevent users from logging on using a stored account password when the conditions for this authentication rule are met. For example, you might want to select Not Allowed to prevent login access when the request comes from an IP address outside of the corporate IP range.
   - You can select **Add New Profile** if you want to create a new authentication profile to use when the selected conditions.

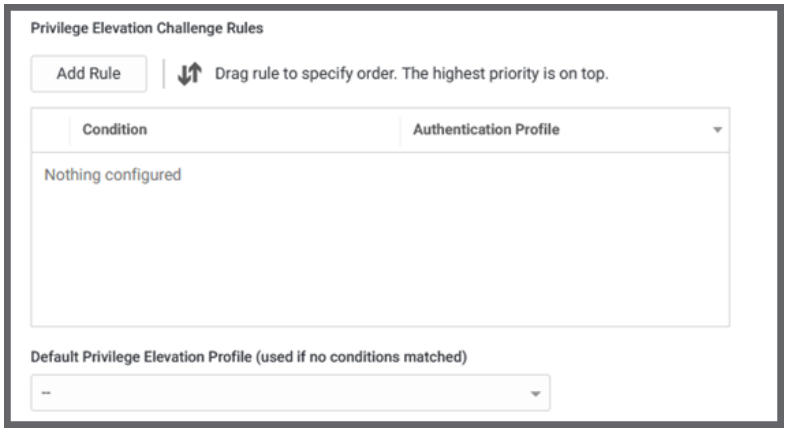
     If you are adding a new authentication profile, type a profile name, select the types of authentication challenges to present, set the challenge duration time to specify how long a previously-satisfied authentication challenge is valid, then click OK. For information about creating authentication profiles and specifying the types of authentication challenges for the authentication profiles you define, see "Creating Authentication Rules" on page 281 and "Creating Authentication Profiles" on page 284.

Privilege Elevation Challenge Rules and Default Profile

For systems and users that you have configured for privilege elevation, you can set up which conditions will result in which additional authentication credentials that users will have to enter when they try to run a privileged command or application. You also specify a default privilege elevation profile that applies if none of the specified conditions are met.

To Configure Privilege Elevation Challenge Rules and Default Authentication Profiles

1. Open the policy tab for the desired systems:
   - One system: In the **Systems** area, open the desired system, then click the **Policy** tab.
   - Some or all systems: In the **Policies** area, open or edit a policy set.
2. In the policy, navigate to **Resources** > **Systems**, and then the **Privilege Elevation Challenge Rules** section of the page.



3. In the **Privilege Elevation Challenge Rules** area, add rules that specify for a particular condition, apply a particular authentication profile.
4. For the **Default Privilege Elevation Profile**, specify which authentication profile applies if none of the conditions in the challenge rules are met.
5. Click **Save** to save your changes.

   The challenge rules and default authentication profile changes for privilege elevation take effect when the affected users next log try to run an application with privilege on an affected system.

Enabling Client Automatic Updates

Select **Yes** to specify that the service automatically updates the Delinea Client software on enrolled systems to the latest client version. After you select Yes, you can also specify a time of day to begin the automatic update.

Setting Domain-Specific Policies

You can set the following domain policy for individual domains or domain sets:

- "Checkout Lifetime" on page 456

To Set Domain-Specific Policies:

1. In the Admin Portal > **Resources** > **Domains** to display the list of domains.
2. Select the domain to display the domain-specific details.
3. Click **Policy**.

4. Select settings for any or all of the domain policies.
5. Click **Save**.

For more information about how to set the domain policies, click the policy link or the information icon in the Admin Portal.

Managing Resources

Managing Accounts

You can manage credentials for both passwords and SSH keys.

Password Management

Centrify Privileged Access Service offers password management by:

- Rotating passwords to a value unknown by humans.
- Password change according to your systems password profile settings.
- Passwords are rotated on a periodic rotation schedule and upon password checkin.

Note: We recommend that privileged account passwords be managed.

SSH Key Management

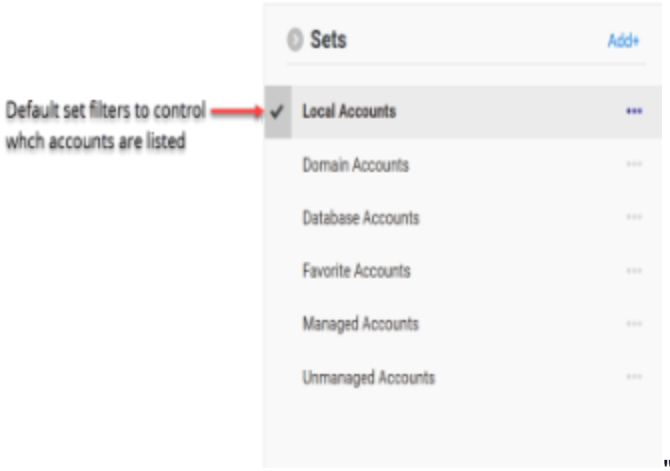
Centrify Privileged Access Service offers SSH key management by:

- Rotating SSH keys, which generates a new key and retires the old key. Once rotated, a new key is added to the SSH keys list and permissions change if the original key was shared.
- New SSH keys are created using specified key algorithm setting.
- SSH keys are rotated on a periodic rotation schedule.

Understanding Account Basics

You can view individual accounts by clicking **Resources** then **Accounts**. The Accounts page lists all of the accounts you have added for managing systems, domains, databases, and services.

You can navigate between different account types by selecting the appropriate set filter. For example, the default account list displays all of the **Local Accounts** you use to access systems such as servers, workstations, and network devices.

" 

"

You can select another filter to see information about a different set of accounts. The information displayed is the same as the information you see under Accounts when you view the details for a specific system, domain, or database.

You can also manage accounts by organizing them into custom groups. Organizing accounts into logical **account sets** simplifies management tasks and reporting for set members.

The Accounts page also provides quick access to the **Multiplexed Accounts** you create for automating password rotation and managing Windows services and scheduled tasks.

If you are a member of a role with the appropriate privilege service rights, you can view, modify, or delete individual accounts or collections of accounts. For more information about performing account-specific tasks, see the following topics:

- "Identifying favorites"
- "Adding account sets"
- "Selecting actions for an account"
- "Management port for password operations"
- "Viewing account details"
- "Changing account settings"
- "Changing access for an account"
- "Viewing password history for an account"
- "Recovering an account password"
- "Enabling request and approval workflow"
- "Setting password checkout policy"
- "Rotating credentials on demand"
- "Setting account permissions"
- "Viewing activity for an account"

- "Deleting accounts"
- "Modifying account sets"

Changing Account Settings

If you are viewing the account details for an individual account, the information you can change depends on the type of system, domain, or database associated with the account. Regardless of the type, however, you cannot change the account name.

For most accounts, you can:

- Select **Manage this credential** to convert an unmanaged account into a managed account. To manage multiple account passwords use the **Manage account** action on the Accounts page.

  You can also right-click a set and select **Manage account** to convert all the accounts associated with the set into managed accounts.
- Deselect **Manage this credential** to convert a managed account into an unmanaged account.
- Select to **Use proxy account**.
- Modify the account description.

If you make any changes to the account, click **Save**.

Settings for Local Accounts

If you are viewing a local account for a Windows, UNIX, or Juniper system, you can also select or deselect **Use proxy account** depending on whether you want to use the proxy account defined for the system. In most cases, you select this option for an account under the following conditions:

- If the target system type is UNIX or Juniper and the root account is not allowed to open secure shell sessions, select this option to use the proxy account defined for the system to start secure shell sessions on the target system.
- If the target system type is Windows and you are using Windows Remote Management to manage passwords, select this option to use the proxy account defined for the system to validate and manage account passwords on the target system.

If you are viewing an account for a generic SSH device, you can edit the account description. You cannot manage account passwords, use a proxy account, or change the account name.

Settings for Multiplexed Accounts

If you are viewing the details for a multiplexed account, you can click Select to change the sub-accounts associated with the account. Before making changes to the sub-accounts for a multiplexed account, however, keep in mind that the sub-accounts must meet the following criteria:

- Each account must be a domain account with its password stored and managed by the Privileged Access Service.
- Each account must have sufficient permissions to run the target Windows service or scheduled task.
- Each account must have Checkout and Edit permission.

- Each account must have the “Log on as a service” user right assigned in a local or domain policy.
- The domain where the sub-accounts are used must have periodic password rotation enabled and an interval set at the domain or global security settings level.

For more information about managing services and automating password rotation, see "Managing Services" on page 680

Changing Account Access

You can change who has access and the permissions associated with an account at any time. For example, if members of the audit role should no longer have access to a target system using a specific account, you can simply delete the role from the list of users and roles allowed to use that account.

To delete users from an account:

1. In the Admin Portal, click **Resources**, then click **Accounts** to display the list of accounts.
2. Select Local Accounts, Domain Accounts, or Database Accounts from the set filters lists to select the type of account you want to modify.
3. Select the specific account from which you want to remove access.
4. From the account details, click Permissions to review the users and roles allowed to use the stored account and the tasks those users and roles are allowed to perform.
5. Select the user, group, or role you want to make ineligible to use the stored account to display the Actions menu for the listed users and roles.

6. Click **Delete**, then click **Save**.

Deleting Accounts

If you have both the Delete and Checkout permissions, you can delete an account from the Privileged Access Service while viewing the accounts stored for a system, domain, or database. For information about setting account permissions to control which users, groups, or roles are allowed to delete accounts, see "Changing Account Access" above

Removing an account from the Privileged Access Service does not affect account information stored locally on the target system, domain, or database. However, you must display or copy the password to the clipboard before the account can be deleted to help ensure you can continue to use the account with its correct password after removing it from the Privileged Access Service.

If you want to delete a system, domain, or database entirely, you must first delete all of the accounts that have been stored for that system, domain, or database.

You can delete one account or bulk accounts as explained below:

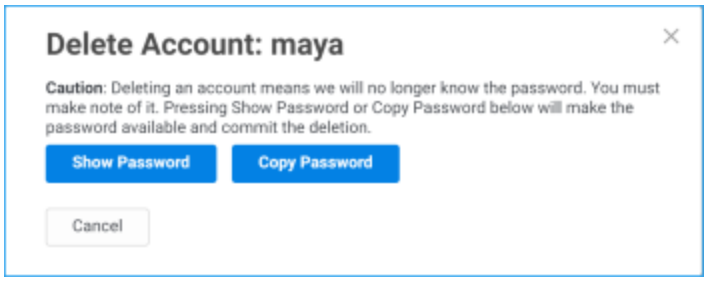
- "To delete an account"
- "To bulk delete accounts"

Deleting a Single Account

1. In the **Admin Portal> Resources >Accounts** to display the list of accounts.
2. Click Local Accounts, Domain Accounts, or Database Accounts to select the type of account you want to delete.
3. Select the specific account you want to delete.

   Optionally, you can display the account details and click Permissions to verify you have the Delete and Checkout permissions. However, you must have the Grant permission to verify permission settings.
4. Click the Actions menu for the account, then click **Delete**.

   For example:

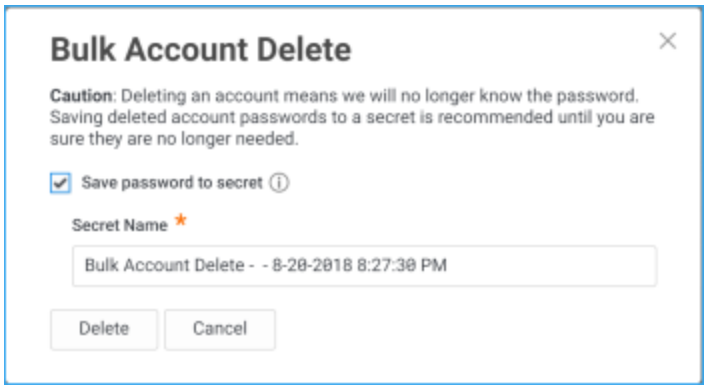


5. Click **Show Password** if you want to view the password for the selected account as plain text or click **Copy Password** to copy the password without viewing it.

   After displaying or copying the password, the account is deleted from the Privileged Access Service immediately.
6. Record the password for future reference, then click **Close**.

Bulk Deleting Accounts

1. In the **Admin Portal> Resources >Accounts** to display the list of accounts.
2. Click Local Accounts, Domain Accounts, or Database Accounts to select the type of account you want to delete.
3. Select the specific accounts you want to delete.
4. Click the **Actions** menu for the account, then click **Delete**.
5. Check the option **Save password to secret** to save the selected account passwords to secret.



You will receive an email notification of the delete activity. Additionally, you can navigate to **Jobs** and review all account activity. Accounts are deleted in the background and may not immediately appear deleted.

Note: If you have performed a bulk account delete, the secret file is saved with view only permission until the system administrator has given you rights to perform additional tasks.

Modifying Account Sets

After you have added an account set, you can modify the details about the set or perform actions on the accounts that are associated with the set. For example, you can:

- Add and remove members
- Change the set name or description
- View recent activity
- Update the permissions on the set
- Rotate passwords for the accounts associated with the set
- Convert unmanaged accounts to managed accounts
- Delete sets

However, you can't modify the membership type setting for existing sets. To change a set from manual membership definition to dynamic or from a dynamic query-based membership definition to manual definition, you must delete the existing set and create a new set.

To modify settings for a account set:

1. In the Admin Portal, click **Resources**, then **Accounts** to display the list of accounts.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Change the set name, set description, or both, as needed.
4. If the membership definition is dynamic, you can modify the set membership by editing the **Query** field.
5. Click **Save**.

For more information about modifying other account set information, see the following topics:

Modifying Set Membership

For manual sets, you can modify the group membership directly from the account list by selecting the account, right-clicking, then selecting the Add to Set or Delete action. To change the set membership if members are defined using a SQL select statement, modify the query in the Settings for the account set.

Viewing Set Activity

You can click Activity to review recent activity for a set. For example, if a user has created, then modified a set, you might see information similar to the following:

When ↓	Detail
06/18/2021 03:15 PM	kimba@centrifystation modified the set membership to the set "Test VMs" of type "Server"
06/18/2021 03:14 PM	kimba@centrifystation modified the set membership to the set "Test VMs" of type "Server"
06/18/2021 03:14 PM	kimba@centrifystation added set "Test VMs" of type "Server"

To view set-specific activity:

1. In the Admin Portal, click **Resources**, then click the section for the type of object you want to view.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Click **Activity**.

Modifying Set Permissions

You can modify the permissions for a set to enable other users to view, edit, or delete the set or to grant permissions on the set to other users. You can assign permissions for the entire set on both manual and dynamic account sets.

The permissions assigned at the set level do not apply to the members of the set. For the members of dynamic account sets, you can only assign member-level permissions through account-specific or global permissions. For manual accounts sets, however, you can assign member-level permissions for all members of the set.

To assign set-level permissions:

1. In the Admin Portal, click **Resources**, then **Accounts** to display the list of accounts.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Click **Permissions**.
4. Click **Add** to search for and select the users, groups, roles, or computers to which you want to grant set-specific permissions, then click **Add**.
5. Select the appropriate permissions for each user, group, role, or computer you have added.
6. Click **Save**.

Modifying Set Member Permissions

You can modify the permissions for the members of a set to control what other users can do on the accounts in the set. For example, you can assign member permissions to enable other users to view, edit, or delete the members of a set or to manage sessions on any member of the set. Member permissions are the same as the permissions you

can assign to individual accounts or globally for all accounts. You can only assign member-level permissions on manual account sets, however.

For more information about the permissions you can assign to accounts, see "Setting Account Permissions" on page 476

To assign member-level permissions:

1. In the Admin Portal, click **Resources**, then **Accounts** to display the list of accounts.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Click **Member Permissions**.
4. Click **Add** to search for and select the users, groups, roles, or computers to which you want to grant set-specific permissions, then click **Add**.
5. Select the appropriate permissions for each user, group, role, or computer you have added.
6. Click **Save**.

Managing Set Accounts

You can convert all unmanaged accounts in a set into managed accounts using the **Manage accounts** action from the Accounts page Sets area.

To manage account passwords in a set:

1. In the Admin Portal, click **Resources**, then **Accounts** to display the list of accounts.
2. In the Sets area, right-click a set name, then click **Manage accounts**.
3. Select **Yes** to confirm that you want to manage passwords for the selected set.
4. You will receive an email notification of the password rotation activity when multiple account passwords are rotated. You can either open the CSV file to view activity or click the link in the email to view the Job History page.

Rotating Set Passwords on Demand

You can rotate all account passwords associated with a set on-demand. For example, if there's suspicious activity involving a particular set of accounts or a risk that a set of accounts has been compromised, you might want to invalidate the existing passwords and have the Privileged Access Service generate a new passwords without waiting for the end of the automated password rotation period.

Note: If you select a set that includes managed and unmanaged accounts, only managed accounts are rotated.

If you rotate a password while an account is currently checked out, the password that has been checked out will no longer be valid and cannot be used to log on or start any new sessions. If there are any existing open sessions that used the checked out password, those sessions can continue.

To rotate passwords in a set on demand:

1. In the Admin Portal, click **Resources**, then **Accounts** to display the list of accounts.
2. In the Sets section, right-click a set name, then click **Rotate passwords**.

3. Select **Yes** to confirm that you want to rotate the selected passwords.
4. Any passwords already checked out are also rotated.
5. You will receive an email notification of the password rotation activity when multiple account passwords are rotated. You can either open the CSV file to view activity or click the link in the email to view the Job History page.

Recovering Account Passwords

If the processing of a password change is interrupted before completion on a target system, the Privileged Access Service will automatically attempt to determine whether the password change was successful or not and recover the appropriate password to use for the account. In a few rare cases, however, the Privileged Access Service might be unable to determine whether the previous or pending password is correct. For example, the following might cause an account to have an indeterminate password if the situation occurs while the Privileged Access Service is processing a password change:

- The network connection to a target system becomes unavailable.
- The target system is shut down.
- There is a service outage on Azure.

If the Privileged Access Service cannot automatically recover the correct password—for example, because the system is still disconnected—you can view details about the most recent password change job and display or copy the last known and pending passwords to try to unlock the account manually. If neither password is correct—for example, because the password has been changed locally on the target system—you can manually reset the password then use the update password feature in the Admin Portal to restore the password in the Privileged Access Service For more information about updating the stored password, see "Updating Passwords for Stored Accounts" on page 665

Understanding Unhealthy Account Statuses

There may be many reasons a password might fail to update on machines stored in Delinea Privileged Access Service. Below is an SQL query that you run on PAS to produce a report with systems and accounts that are failing password rotation.

To run the report

1. Navigate to the Delinea PAS > **Reports** > **New Report**.
2. Build a new report using the editor.
3. Paste the SQL query, **AccountsNotRotating.sql**, into the editor.

   "SQL query"
4. **Save** and **Run** the report.
5. From the **Actions** in the report results, export the report. The report can be saved as an Excel or CSV file.

Interpreting the report results

The status of a machine and its accounts are determined by opening the report in Microsoft Excel and reviewing the report column headers in row one. The columns that are considered are:

- SystemHealthStatus (C)
- AccountHealthError (I)
- PasswordResetRetryCount (K)
- PasswordResetLastError (L)
- SystemManagementMode (Q)
- SystemComputerClass (P)
- AccountNeedsPasswordReset (J)

Report columns and values	Result status	Follow up actions
SystemHealthStatus is Unreachable.	System Unreachable	If the system is no longer in service, consider deleting it.. Check if the machine is "pingable." Verify DNS is correctly resolving the name as it appears in the "DNS Name/IP Address" of the system in PAS.
SystemHealthStatus is OK.AccountHealthError is BadCredentials.PasswordResetLastError is 'System error'.	Password Needs Updating	The password in not being rotated because the current password is unknown.Reset the password on the target machine Update the password in PAS. Manually rotate the password. The password should rotate automatically going forward.

Report columns and values	Result status	Follow up actions
SystemHealthStatus is OK. AccountHealthError is OK. PasswordResetRetryCount > 0 SystemManagementMode is RpcOverTcp PasswordResetLastError is HostNotFound.	RPC Dynamic Ports Blocked	The machine has an open port that permits the account to be validated OK, but does not have the RPC dynamics ports open which are needed to rotate the password. The RPC dynamic ports are 49152 - 65535. Adjust the firewall to open the dynamic RPC ports. Manually rotate the password.
SystemHealthStatus is OK. AccountHealthError is OK. PasswordResetRetryCount > 0 PasswordResetLastError is 'User has no SAM remote access rights'.	SAM Remote Access Restriction	On newer versions of Windows, access to the Windows authentication database is restricted and prevents password rotation.Update the local security policy of the target machine: **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options** > **Network access: Restrict clients allowed to make remote call to SAM Add the account name to the policy**. Manually rotate the password.

Report columns and values	Result status	Follow up actions
SystemHealthStatus is OK. AccountHealthError is OK. PasswordResetRetryCount > 0 SystemComputerClass is UnixAccount NeedsPasswordReset is RetryLimitExceeded	Unix System Offline for Too Long	The machine has been offline for a long time, but the system and accounts are OK. Manually rotate the password. The password should rotate automatically going forward.
SystemHealthStatus is OK. AccountHealthError is OK. PasswordResetRetryCount = 0	Needs More Investigation - No Attempt to Rotate Password	This machine needs more investigation. Manually rotate the password. If the password does not rotate, gather the tenant logs, collector logs, time stamp, and account information for further analysis.
SystemHealthStatus is OK. AccountHealthError is OK. PasswordResetRetryCount > 0 SystemManagementMode is Smb PasswordResetLastError is HostNotFound.	Needs More Investigation - SMB	This machine needs more investigation. Manually rotate the password. If the password does not rotate, gather the tenant logs, collector logs, time stamp, and account information for further analysis.
SystemHealthStatus is OK. AccountHealthError is OK. PasswordResetRetryCount > 0 SystemManagementMode is Smb. PasswordResetLastError is AccountRestrictionsPreventSignin	Needs More Investigation - AccountRestrictionsPreventSignin	There is some restriction on the target machine preventing password rotation. Investigate any password restrictions on target machine. Gather the tenant logs, collector logs, time stamp, and account information for further analysis.

Report columns and values	Result status	Follow up actions
SystemHealthStatus is OK. AccountHealthError is BadCredentials PasswordResetLastError is HostNotFound.	Password Needs Updating and RPC Dynamic Ports Blocked	This machine's account needs both a password update and unblocking of the RPC dynamic ports. Adjust the firewall to open the dynamic RPC ports.s (949152 - 65535) Reset the password on the target machine. Update the password in Delinea PAS. Manually rotate the password.
SystemHealthStatus is OK. AccountHealthError is OK. PasswordResetRetryCount > 0 PasswordResetLastError is 'Password policy is violated'.	Password Policy	The system has a password policy that is more restrictive than the passwords generated by Delinea PAS. Check the password policy for local accounts.

Viewing Account Activity

You can click Activity to review recent activity, such as password check out and check in activity or remote access to a target, for the selected account.

To view account-specific activity:

1. Select the **Resources**, then select **Accounts** to display the list of accounts.
2. Select an account to display the account details.
3. Click **Activity**.

Viewing Account Details

Clicking an account name in the Local Accounts, Domain Accounts, Database Accounts, or Multiplexed Accounts list displays the account details. From the account details, you can click the Actions menu to perform the account-related tasks or make changes to the account settings.

For most accounts, you have the following options:

- **Account settings** to specify whether the account password is managed by the Privileged Access Service, whether the account uses a proxy account, and to change or update the account description. For more information, see "Changing Account Settings" on page 647

- **Password history** to review the password history for an account. For more information, see "Viewing Account Password History" below
- **Policy** to set account-specific policies. For more information, see "Setting Password Checkout Policy" on page 477
- **Workflow** to enable an account-specific “request and approval” work flow. For more information about enabling a “request and approval” work flow, see "Request and Approval Workflow Overview" on page 774
- **Permissions** to specify the users who are authorized to use the account and what each user is allowed to do. For more information, see "Changing Account Access" on page 648
- **Activity** to view details about the activity performed by users who have accessed an account. For more information, see "Viewing Account Activity" on the previous page

For more information about the actions available when you select an account, see "Account Password Checkout" on page 460

Viewing Account Password History

Depending on the administrative rights and permissions granted to your account, you can view the password history and the specific passwords that have been used for accounts that are stored in the Privileged Access Service. For example, if you are a member of a role with Privilege Service Power User rights but have not been granted the Checkout permission, you can view the list of password changes that have been recorded in the Privileged Access Service but not display the password strings that have been used. If you are using an account that includes the Checkout permission, however, you can use the password history to recover a previously-used password for an account, then use that password, if needed, to access a system.

The password history lists all password change events for an account, regardless of whether they are caused by automatic password rotation, by checking in a managed password, or by manually updating the password for an unmanaged account. Each time a password is retired, the password history is updated with a new event that records the password that has been retired.

To view the password history for an account:

1. In the Admin Portal, click **Resources**, then click **Accounts** to display the list of accounts.
2. Click Local Accounts, Domain Accounts, or Database Accounts to select the type of account for which you want to view password history.
3. Select the specific account for which you want to review password history.
4. From the account details, click **Password History**.

   The password history lists the date and time of each password change event and the user who checked the password in, causing the old password to be replaced with a new password. If the password checkout period expired or the password was changed automatically because of a password rotation policy, the Retired by column displays SYSTEM$ to indicate the password change was initiated internally by the Privileged Access Service.
5. Select the password change event in which you are interested, then select **View Password** from the Actions menu.

Note that this action is only available if you have Checkout permission for the account and system combination you are viewing.

Click **Show Password** if you want to view the password for the selected account as plain text or click **Copy Password** to copy the password without viewing it.

6. The checkout is recorded as recent activity in the dashboard and in the list of system activity.
7. Click **Close**.

By default, the Privileged Access Service automatically removes the oldest retired passwords from the password history after 365 days. You can use system-specific policies to change the interval at which the Privileged Access Service automatically removes retired passwords or to prevent the Privileged Access Service from automatically removing any retired passwords. For more information about setting the system policies for password cleanup, see "Enabling Periodic Password History Cleanup" on page 485

Rotating Credentials on Demand

In most cases, you configure automatic credential rotation for managed accounts by setting policies globally or for individual Systems, domains, or databases. In order to successfully rotate an account password, you must have the rotate permission for the accounts you want to rotate.

There are scenarios, however, where you might want to generate a new credential for an account or multiple accounts on demand. For example, if there's suspicious activity involving a particular account(s) or a risk that an account or set of accounts has been compromised, you might want to invalidate the existing credential and have the Privileged Access Service generate a new credential without waiting for the end of the automated credential rotation period.

You can select to rotate credentials for one or multiple individual managed accounts or you can select all accounts associated with a set. If you select multiple accounts or a set that includes managed and unmanaged accounts, only managed accounts are rotated.

If you rotate a credential while an account is currently checked out, the credential that has been checked out will no longer be valid and cannot be used to log on or start any new sessions. If there are any existing open sessions that used the checked out credential, those sessions can continue.

SSH Key-based Accounts

When an SSH key-based account is shared and rotated, it changes permission on that SSH key. For example: once the SSH key is rotated, a user who previously had permission to the shared SSH key will no longer have permission once the key is rotated. Once rotated, the shared key is replaced with a new key for the account.

The following steps detail how you can rotate passwords or SSH keys on demand.

Rotating Credentials on Demand

1. In the Admin Portal, click **Resources**, then click **Accounts** to display the list of accounts.
2. In the Sets section, click **Managed Accounts** to filter the list of accounts displayed.
3. Select the managed account or multiple managed accounts requiring password rotation. You can also select all accounts associated with the set.

4. Click the **Actions** menu or right-click the **Set**. For accounts with passwords, select **Rotate Password**. For accounts using SSH keys, select **Rotate SSH Key**.
5. Select **Yes** to confirm that you want to rotate the selected passwords. Any passwords already checked out are also rotated. You will receive an email notification of the password rotation activity when multiple account passwords are rotated. You can either open the CSV file to view activity or click the link in the email to view the Job History page.

Note: When an SSH key is rotated, the permissions on the key change. After rotation, permissions default to minimum required settings. Permissions are not duplicated.

Managing Databases

Individual databases can be viewed by clicking **Resources > Databases**. The Databases list includes all of the databases available for you to manage. If you are a member of a role with the appropriate administrative rights, you can view, add, or delete databases and database accounts from this list.

Modifying Database-specific Details

When you are viewing the details for an individual database, you can also change database settings, view and add account information, define database-specific policies, and review recent logon and password activity. For more information about viewing and modifying database-specific information, see the following topics:

- "Adding Database Accounts" below
- "Changing Database Settings" on page 666
- "Selecting Connectors" on the next page
- "Setting Database-specific Permissions" on page 664
- "Setting Database-specific Policies" on page 664
- "Updating Passwords for Stored Accounts" on page 665
- "Viewing Database Activity" on page 666
- "Viewing Database Accounts and Account Activity" on page 665

Adding Database Accounts

If you skipped the step for adding a database account when you added or imported a database, provided invalid account information when you added the database, or want to update the database to include additional accounts, you can do so after adding the database by clicking **Accounts** when viewing the details for the database.

To add a new account for a database:

1. In the Admin Portal, click **Resources > Databases** to display the list of databases.
2. Select the database to display the database-specific details.
3. Click Accounts, then click **Add**.
4. Type the user name and password for a database account you want to use to connect to the currently selected database.

5. Select the **Manage this credential** option if you want the Delinea Privileged Access Service to manage the password for the specified account.
6. Optionally, type a description for the account, then click **Add**.
7. Click **Save** to save the new account for the database.

Managing Passwords and Password Complexity

For any database account you add, you can also choose whether or not you want the Privileged Access Service to manage the account password. If you select **Manage this credential**, the Privileged Access Service automatically resets the password after the account and database are added and each time the account is checked in.

All managed passwords generated by the Privileged Access Service consist of at least one upper case letter, one lower case letter, one number, and one special character regardless of the database type.

The default password profile for each database type will only include supported special characters. If you clone an existing profile to create a custom password profile, however, you should be aware that some special characters might not be supported on different databases and should not be used in the password.

For example, the following password rules apply when adding **Microsoft SQL Server** database accounts:

- Minimum password length: 12 characters.
- Maximum password length: 32 characters.
- Supported special characters: ?!@#$%&()*+,-./:<=>[]^_|~

For **Oracle** database accounts, the following password rules apply:

- Minimum password length: 12 characters.
- Maximum password length: 30 characters.
- Supported special characters: !@#$%&()*+,-./:;<=>?[]^_{|}~
- Only characters that are standard ASCII characters are supported.

If you are adding database accounts for **SAP Adaptive Server Enterprise**, the following password rules apply:

- Recommended minimum password length is 6 characters.
- Maximum password length is 30 characters

User names and passwords cannot begin with single quotes or double quotes.

User names and passwords cannot end with white space.

You can also implement advanced password rules that include requiring certain types of characters in the password, disallowing password reuse, and determining when passwords should expire.

You should keep in mind that only the Privileged Access Service will know the managed password being generated and stored. You should not select this option if you don't want the Privileged Access Service to manage the password for the account.

Selecting Connectors

By default, database connections use any available connector without evaluating the network topology. If the communication with a current connector is interrupted, the database connection will automatically select another

available connector to continue operation. To give you more control over which connector different databases use, you can choose one or more database-specific connectors.

If you want to specify the connectors for an individual database, you can do so when viewing the details for the database. Database-specific settings take precedence over any global connector subnet mapping you might have configured.

To specify the connectors to use for a database:

1. In the **Admin Portal > *Resources* > Databases** to display the list of databases.
2. Select the database to display the database-specific details.
3. Click **Connectors**.
4. Select **Choose**, then select the connectors to use for the database from the list of available connectors.
5. Click **Save**.

Setting Database-specific Advanced Options

You can set advanced security and maintenance settings for individual databases or database sets. You can also set security and maintenance options globally to apply to all databases except where you have explicitly defined a database-specific setting. If you use a combination of global and database-specific settings, the database-specific settings take precedence over the global settings.

If you are not using global security settings or want to override global settings on specific databases, you can set the following advanced security and maintenance options on a case-by-case basis:

- "Allow multiple password checkouts"
- "Enable periodic password rotation"
- "Enable password rotation after checkin"
- "Minimum password age"
- "Password complexity profile"
- "Enable periodic password history cleanup"

To set database-specific advanced options:

1. In the Admin Portal, click **Resources**, then click **Databases** to display the list of databases.
2. Select the database to display the database-specific details.
3. Click **Advanced**.
4. Select settings for any or all of the advanced database options.
5. Click **Save**.

For more information about how to set the database-specific options, click the information icon in the Admin Portal.

Allowing Multiple Password Checkouts

- Select **No** if only one administrator is allowed check out the password for a selected database account at any given time. If you select No, the administrator must check the password in and have a new password generated before another administrator can access the database with the updated password.
- Select **Yes** if you want to allow multiple users to have the database account password checked out at the same time for a selected database. If you select Yes, multiple administrators can check out the password for the database without waiting for the account password to be checked in.

Enabling Periodic Password Rotation

- Select **Yes** if you want to rotate managed passwords automatically at the interval you specify.
- Select **No** if you want to prevent password rotation for the selected database.
- If you select **Yes**, you should also specify the **Password rotation interval** in days. Type the maximum number of days to allow between automated password changes for managed accounts. You can set this policy to comply with your organization's password expiration policies. For example, your organization might require passwords to be changed every 90 days. You can use this policy to automatically update managed passwords at a maximum of every 90 days. If the policy is not defined, passwords are not rotated.

Enabling Password Rotation after Check-in

After you check out a managed password for a database, you can specify whether the managed password is rotated after it is checked in.

Select **Yes** to allow password rotation after password check in. Select **No** to not allow password rotation after it is checked in. Select ***--*** to use the default setting from the Security Settings in the Settings tab.

Setting the Minimum Password Age

Specify the minimum number of days that a managed password must have been in use before it can be rotated.

Password Complexity Profile

Select an existing password generation profile or add a new profile for the selected database. If you don't select or add a profile, the default password generation profile for the database type is used. For more information about adding and editing password complexity profiles, see "Configuring Password Profiles" on page 751

Enabling Periodic Password-History Cleanup

- Select **Yes** to automatically delete retired passwords from the password history after a given number of days.
- Select **No** to prevent the from automatically deleting retired passwords from the password history at a set interval.
- If you select yes, you can also specify the maximum number of days of password history to keep. For example, if you have a requirement to keep a record of passwords used for three years, you might set the cleanup interval to 1096 days to maintain the password history for that period of time. If you select the default setting, retired passwords are automatically deleted after 365 days. You cannot set a cleanup interval less than 90 days.

Setting Database-specific Permissions

You can set permissions for individual databases or on the members of a set of databases. You can also set account permissions for the accounts used to access databases.

To set database-specific permissions:

1. In the **Admin Portal > Resources > Databases** to display the list of databases.
2. Select the database to display the database details.
3. Click **Permissions**.
4. Click Add to search for and select the users, groups, or roles to which you want to grant database-specific permissions, then click **Add**.
5. Select the appropriate permissions for each user, group, or role you have added, then click **Save**.

For more specific information about what different permissions allow users to do, see "Assigning Permissions" on page 743

Setting Database-specific Policies

Setting Policies

You can set the following policy for individual databases or database sets.

To set database-specific policies:

1. In the **Admin Portal > Resources > Databases** to display the list of databases.
2. Select the database to display the database-specific details.
3. Click **Policy**.
4. Select settings for any or all of the database policies.
5. Click **Save**.

For more information about how to set the databases-specific policies, click the policy link or the information icon in the Admin Portal. If you set polices globally, the global policies apply by default to all database accounts except where you have explicitly defined a database-specific policy.

Checkout Lifetime

Type the maximum number of minutes administrators are allowed to have a database account password checked out. After the number of minutes specified, the Privileged Access Service automatically checks the password back in. The minimum checkout lifetime is 15 minutes. If the policy is not defined, the default checkout lifetime is 60 minutes.

You can extend the checkout time for a password as long as you do so before the initial checkout period expires. For example, if the maximum checkout lifetime is 60 minutes and you extend the checkout time before the 60 minute period is over, the password expiration is reset to the 60 minute checkout lifetime. For more information about configuring the Checkout lifetime policy, see "Extending Password Checkout Time" on page 464

Updating Passwords for Stored Accounts

If you change the password for any stored account locally on a target database, the account password stored in the Privileged Access Service will no longer be valid. Because the password stored in the Privileged Access Service no longer matches the password that has been changed for the database, you will not be able to use the stored password.

To synchronize the passwords so that the current password can be checked out and used to log on, you must update the password stored in the Privileged Access Service. You can update the password for managed or unmanaged accounts from the Accounts page by selecting an account or by clicking **Accounts** when viewing the details for the database.

To update the password for a stored account

1. In the **Admin Portal** > **Resources** > **Databases** to display the list of databases.
2. Select the database to display the database-specific details.
3. Click **Accounts**.
4. Select the account that no longer has a valid password stored in the Privileged Access Service.
5. Click the Actions menu, then select **Update Password**.

   The Update Password action is available for both managed and unmanaged accounts. In both cases, be sure you have the correct current password for the account. If you are unsure, reset the password on the target database first, then update the password stored in the Privileged Access Service.
6. Type the current password for the account you are updating.

   You should update the password stored in the Privileged Access Service any time the password for an account has been changed locally on the target database. You also might need to update the password if a network failure or other event occurs and the password cannot be recovered automatically.

   Note that updating the stored password for an unmanaged account does not change any information on the target database. If you type the wrong password or have not yet changed the password for the selected account on the database, you will not be able to use the account to connect to the database.

   If you are updating the stored password for a managed account, reset the password for the database account first. After you save the updated password that matches the reset password, the Privileged Access Service validates the account information then generates a new managed password and changes the account password to the newly-generated password. For more information about recovering lost passwords, see "Recovering Account Passwords" on page 653)
7. Click **Save** to save the new password for the account.

Viewing Database Accounts and Account Activity

In most cases, you add the database account for connecting to a database when you initially add the database to the Privileged Access Service. From the list of Accounts for a database, you can then view the following information:

- User Name indicates the name the account uses to access the database.
- Last reset specifies the date and time the database account password was last reset.

- Checkouts specifies the number of password checkouts for the database account.
- Last Verify Result indicates the result of the most recent password check for an account. If the password stored by the Privileged Access Service is no longer valid, the column displays Failed. If the state of the password cannot be determined—for example, because the account is an unmanaged account—the column displays Unknown.
- Last Verify displays the date and time of the last password verification.
- Managed displays a check mark if the password for the account is managed through the Privileged Access Service.

From the list of database accounts for a specific database, you can add, modify, or delete the accounts used to access that database.

When you are viewing the accounts for a database, you can also select any account in the list, then click the Actions menu to check out the password for the account, update the password stored in the Privileged Access Service for the account, or delete the account.

Viewing all Database Accounts

You can view the accounts that have been added for individual databases from the database details. To see a list of all database accounts for all databases in the Privileged Access Service, you can click **Resources**, then click **Accounts** and select **Database Accounts**.

From the Database Accounts list, you can search for database accounts across all databases. You can also select an individual account for any database to perform account-related actions—such as check out an account password or update the account's stored password. The information displayed on the Database Accounts list is the same as the information displayed for accounts when you are viewing the details for a specific database.

Viewing Database Activity

You can click Activity to review recent activity, such as password check out and check in activity, for the selected database and database account. For example, if a user has successfully logged on to the selected database using a stored database account, checked out or checked in an account password, and had a failed logon attempt, you can see details about the event.

To view database-specific activity:

1. In the Admin Portal > ***Resources*** > **Databases** to display the list of databases.
2. Select the database to display the database-specific details.
3. Click **Activity**.

Changing Database Settings

You can click **Database Settings** page to do the following:

- Change the display name, host name, or IP address for a previously added database
- Specify the port number used to check the status of the database
- Change the service name or instance name of the database when updating database passwords

- Add or modify an optional description for the selected database
- Add certificates to SAP ASE Databases by either uploading the certificate or entering it manually.

Deleting Database Accounts

You can remove an database account for a database from the Privileged Access Service at any time. Before you can remove a database account, however, you must display or copy the password to the clipboard before the account can be deleted to help ensure you can continue to use the account with its correct password after removing it from the Privileged Access Service.

To remove a database account:

1. In the **Admin Portal> Resources > Databases** to display the list of databases.
2. Select a database to display the database details.
3. Select the database account, then click the **Actions** menu.
4. Click **Delete**.
5. Click **Show Password** if you want to view the password for the selected account as plain text or click **Copy Password** to copy the password without viewing it.

   After displaying or copying the password, the account is deleted immediately.
6. Record the password for future reference, then click **Close**.

Deleting Databases

You can remove a database from the Databases list and the Privileged Access Service only if you have removed all database accounts for the database.

To remove a database from the service:

1. In the **Admin Portal > Resources > Databases** to display the list of databases.
2. Select a database to display the database details.
3. Select Accounts to verify that there are no database accounts associated with the database.
4. Click the Actions menu, then click **Delete**.
5. Click **Yes** to confirm that you want to proceed with deleting the database.

Modifying Database Sets

After you have added a database set, you can modify the details about the set at any time. For example, you can add and remove members, change the set name or description, view recent activity, or update the permissions on the set.

However, you can't modify the membership type setting for existing sets. To change a set from manual member definition to dynamic or from a dynamic query-based member definition to manual definition, you must delete the existing set and create a new set.

To modify settings for a database set:

1. In the Admin Portal, click **Resources**, then click **Databases** to display the list of databases.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Change the set name, set description, or both, as needed.
4. If the membership definition is dynamic, you can modify the set membership by editing the **Query** field.
5. Click **Save**.

For more information about modifying other database set information, see the following topics:

- "Modifying Database Sets" on the next page
- Viewing Set Activity
- "Modifying Set Permissions" below
- "Modifying Set Member Permissions" below

Modifying Set Member Permissions

You can modify the permissions for the members of a set to control what other users can do on the databases in the set. For example, you can assign member permissions to enable other users to view, edit, or delete the members of a set or to manage sessions on any member of the set. Member permissions are the same as the permissions you can assign to individual databases or globally for all databases. You can only assign member-level permissions on manual databases sets, however.

For more information about the permissions you can assign to databases, see "Setting Database-specific Permissions" on page 664

To assign member-level permissions:

1. In the Admin Portal, click **Resources**, then click **Databases** to display the list of databases.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Click **Member Permissions**.
4. Click **Add** to search for and select the users, groups, or roles to which you want to grant set-specific permissions, then click **Add**.
5. Select the appropriate permissions for each user, group, or role you have added.
6. Click **Save**.

Modifying Set Permissions

You can modify the permissions for a set to enable other users to view, edit, or delete the set or to grant permissions on the set to other users. You can assign permissions for the entire set on both manual and dynamic database sets. The permissions assigned at the set level do not apply to the members of the set. For the members of dynamic database sets, you can only assign member-level permissions through database-specific or global permissions. For manual databases sets, however, you can assign member-level permissions for all members of the set.

To assign set-level permissions:

1. In the Admin Portal, click **Resources**, then click **Databases** to display the list of databases.
2. In the Sets section, right-click a set name, then click **Modify**.

3. Click **Permissions**.
4. Click **Add** to search for and select the users, groups, or roles to which you want to grant set-specific permissions, then click **Add**.
5. Select the appropriate permissions for each user, group, or role you have added.
6. Click **Save**.

Modifying Database Sets

After you have added a database set, you can modify the details about the set at any time. For example, you can add and remove members, change the set name or description, view recent activity, or update the permissions on the set.

However, you can't modify the membership type setting for existing sets. To change a set from manual member definition to dynamic or from a dynamic query-based member definition to manual definition, you must delete the existing set and create a new set.

To modify settings for a database set:

1. In the Admin Portal, click **Resources**, then click **Databases** to display the list of databases.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Change the set name, set description, or both, as needed.
4. If the membership definition is dynamic, you can modify the set membership by editing the **Query** field.
5. Click **Save**.

For more information about modifying other database set information, see the following topics:

- "Modifying Database Sets" above
- "Modifying Database Sets" on page 667
- "Modifying Set Permissions" on the previous page
- "Modifying Set Member Permissions" on the previous page

Selecting Databases

You can select a database to work with by clicking anywhere in the row that contains the database name to display the database details or by clicking the check box for a row. Selecting a database displays the Actions menu. From the Actions menu, you can click:

- **Add to Set** to add the selected system to a new or existing set.
- **Delete** to remove a database from the list.
- **Test connection** to perform a check on the selected database and determine if the database is reachable. The Test connection function is not supported for the SQL Server database type if a port number is not specified.

You can also select an action from the Actions menu when viewing the details for an individual database or view and modify database-specific information. For example, when you are displaying the details for a selected database, you can do the following:

- Change database settings such as the database name and description.
- Add database accounts and view database account activity, such as the date and time of the last password reset and the number of active sessions for the account.
- Specify the connectors to use for the database.
- Set database-specific policies.
- View recent activity for the database, such as who has checked out or checked in a password for database accounts.
- Set database-specific permissions for the users who are allowed to access the database with stored accounts.

Setting Database-Specific Policies

You can set the following policy for individual databases or database sets:

"Checkout Lifetime" below

To Set Database-Specific Policies:

1. In the **Admin Portal > Resources > Databases** to display the list of databases.
2. Select the database to display the database-specific details.
3. Click **Policy**.
4. Select settings for any or all of the database policies.
5. Click **Save**.

For more information about how to set the databases-specific policies, click the policy link or the information icon in the Admin Portal. If you set polices globally, the global policies apply by default to all database accounts except where you have explicitly defined a database-specific policy.

Checkout Lifetime

Type the maximum number of minutes administrators are allowed to have a database account password checked out. After the number of minutes specified, the Privileged Access Service automatically checks the password back in. The minimum checkout lifetime is 15 minutes. If the policy is not defined, the default checkout lifetime is 60 minutes.

You can extend the checkout time for a password as long as you do so before the initial checkout period expires. For example, if the maximum checkout lifetime is 60 minutes and you extend the checkout time before the 60 minute period is over, the password expiration is reset to the 60 minute checkout lifetime. For more information about configuring the Checkout lifetime policy, see "Extending Password Checkout Time" on page 464.

Viewing Databases

After you have added at least one database, you can click the Databases tab to view the following information for all databases:

- Name is the unique name you use to identify the database.
- Hostname is the fully-qualified server name or IP address that hosts the database.

- Type specifies the type of database being hosted.
- Last Test Result displays nothing if the account used to connect to the database was successful. If the connection to the database failed for any reason—for example, because the account name and password are invalid or a network connection to the database is not available, or if there is no database account—the column displays Unreachable or Unknown.
- Last Test displays the date and time of the last database health check. A health check is performed when Test connection is selected from the Actions menu or when a database is added to Privileged Access Service.

Managing Domains

Individual domains can be viewed by clicking **Resources > Domains**. The Domains list includes all of the Active Directory domains available for you to manage that you have added to the Privileged Access Service.

You can populate this list automatically for selected domains by running discovery jobs. Discovery enables you to create a profile to identify the domains in which you are interested, then scan the network for domains that match the criteria you have specified. You can also add domains without running discovery jobs by adding them manually.

You can also manage domains by organizing them into groups. Organizing domains into logical **domain sets** simplifies management and reporting for set members.

If you are a member of a role with the appropriate privilege management rights, you can view, add, modify, or delete individual domains in the **Domains** list or collections of member domains in the **Sets** list. If you are the owner of a domain or a domain set because you added it to the Privileged Access Service, you can grant permissions to other users, groups, and roles to work with the domain or domain set you own.

Deleting Domains

You can remove a domain from the Domains list and the Privileged Access Service only if you have removed all account information for the domain.

To remove a domain from the Privileged Access Service

1. In the **Admin Portal > Resources > Domains** to display the list of domains.
2. Select a domain from the domain list to display its details.
3. Select Accounts to verify that there are no accounts associated with the domain.
4. Click the Actions menu, then click **Delete**.
5. Click **Yes** to confirm that you want to proceed with deleting the domain.

Modifying Domain Sets

After you have added a domain set, you can modify the details about the set at any time. For example, you can add and remove members, change the set name or description, view recent activity, or update the permissions on the set.

However, you can't modify the membership type setting for existing sets. To change a set from manual membership definition to dynamic or from a dynamic query-based membership definition to manual definition, you must delete the existing set and create a new set.

To modify settings for a system set:

1. In the Admin Portal, click **Resources**, then click **Domains** to display the list of domains.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Change the set name, set description, or both, as needed.
4. If the member definition is dynamic, you can modify the set membership by editing the **Query** field.
5. Click **Save**.

For more information about modifying other domain set information, see the following topics:

- "Modifying Database Sets" on page 669
- Viewing Set Activity
- "Modifying Set Permissions" on page 682
- Modifying Member Permissions for a Set

Modifying Set Member Permissions

You can modify the permissions for the members of a set to control what other users can do on the domains in the set. For example, you can assign member permissions to enable other users to view, edit, or delete the members of a set or to manage sessions on any member of the set. Member permissions are the same as the permissions you can assign to individual domains or globally for all domains. You can only assign member-level permissions on manual domain sets, however.

For more information about the permissions you can assign to systems, see "Setting Domain-specific Permissions" on page 490

To assign member-level permissions:

1. In the Admin Portal, click **Resources**, then click **Domains** to display the list of domains.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Click **Member Permissions**.
4. Click **Add** to search for and select the users, groups, roles, or computers to which you want to grant set-specific permissions, then click **Add**.
5. Select the appropriate permissions for each user, group, role, or computer you have added.
6. Click **Save**.

Modifying Set Membership

For manual sets, you can modify the group membership directly from the domain list by selecting the domain, right-clicking, then selecting the Add to Set or Delete action. To change the set membership if members are defined using a SQL select statement, modify the query in the Settings for the domain set.

Modifying Domain Sets

After you have added a domain set, you can modify the details about the set at any time. For example, you can add and remove members, change the set name or description, view recent activity, or update the permissions on the set.

However, you can't modify the membership type setting for existing sets. To change a set from manual membership definition to dynamic or from a dynamic query-based membership definition to manual definition, you must delete the existing set and create a new set.

To modify settings for a system set:

1. In the Admin Portal, click **Resources**, then click **Domains** to display the list of domains.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Change the set name, set description, or both, as needed.
4. If the member definition is dynamic, you can modify the set membership by editing the **Query** field.
5. Click **Save**.

For more information about modifying other domain set information, see the following topics:

- "Modifying Database Sets" on page 669
- Viewing Set Activity
- Modifying Permissions for a Set
- "Modifying Set Permissions" on page 682

Selecting and Updating Domains

You can select a domain to work with by clicking anywhere in the row that contains the domain name to display the domain details.

After you display the details for a selected domain, you can also change the domain description, add accounts from the domain to the Privileged Access Service, specify the domain-specific connectors to use, set domain-specific policies, view recent activity for the domain, and set domain-specific permissions.

To update a domain name or description:

1. In the Admin Portal, click **Resources**, then click **Domains** to display the list of domains.
2. Select a domain and click **Settings** to display the domain name and description.
3. Type a new name for the domain if you added the wrong domain name and skipped verification of connectivity.
4. Type a new description for the domain, then click **Save**.

Testing Domain Connections

Select **Test connection** from the **Actions** menu to check the connection to a domain or multiple domains and determine if the it is reachable.

To test the domain connection:

1. In the **Admin Portal > Resources > Domains** to display the list of domains.
2. Select a domain or multiple domains from the domain list to display its details.
3. Click the **Actions** menu, then click **Test connection**.

Viewing and Searching Domains

After you have added at least one domain, you can click Domains to view the list of domain names and the current status of each domain. To search for a specific domain, type all or part of the domain name in the Search field.

If you have added any manual or dynamic domain sets, they are added as filters in the Sets section. You can then use the predefined and custom set filters to select domains that match specific criteria, such as a custom query or a manual membership you have defined.

In addition to the filters for the sets you have created, you can also filter the list of domains displayed by typing a search string, or by combining a set filter and a search string.

After you have added at least one domain, you can click the Domains tab to view the following information for all added domains:

- Domain Name is the unique name you use to identify the domain.
- Last Test Result displays nothing if the account used to connect to the domain was successful. If the connection to the domain failed for any reason—for example, because the network connection to the domain is not available—the column displays Unreachable or Unknown.
- Last Test displays the date and time of the last domain health check. A health check is performed when Test connection is selected from the Actions menu or when a domain is added to Privileged Access Service.
- Administrative Account displays the name of the Administrative Account for the domain if configured. See "Setting Domain Admin Accounts" on page 493
- Discovered displays a time stamp, if the domain was added during the discovery process. The time stamp indicates the time the domain was added. If the domain was added using a different method, such as manually or using the import process, nothing is displayed. Auto is displayed if the domain is automatically synced with an active connector.

Viewing Domain Account Info

After you add an account to the domain, you can then view the following information:

- Last reset specifies the date and time the account password was last reset.
- Sessions specifies the number of currently active sessions for the account.
- Checkouts specifies the number of password checkouts for the account.
- Last Verify Result indicates the result of the most recent password check for an account. If the password stored by the Privileged Access Service is no longer valid, the column displays Failed. If the state of the password cannot be determined—for example, because the port used to check account health is blocked, the account is in an untrusted forest, or the account is an unmanaged account—the column displays Unknown.
- Last Verify displays the date and time of the last password verification.
- Managed displays a check mark if the password for the account is managed through the Privileged Access Service.

When you are viewing the accounts for a domain, you can also select any account in the list, then click the Actions menu to log on to a domain computer using the stored account password, check out the password for the account, log on to a domain computer using the stored password for the account, update the account password, or delete the account.

For more information about performing these tasks, see the following topics:

- "Checking out an account password"
- "Checking in a password"
- "Updating the password for a domain account"
- "Viewing all domain accounts"

Checking in Passwords

After you check out a password, you have a limited period of time in which the password you checked out is valid for activity on a domain computer. If the Privileged Access Service manages the password for the account, you should check in the password when you end the session, so that a new secure password can be generated for the account you used.

You can check in a password you have previously checked out from the Accounts list when viewing domain details, the Accounts tab directly, or the Workspace tab. For more information about working with accounts directly, see "Managing Accounts" on page 645 For more information about checking in passwords while reviewing the summary of your activity, see "Checking in Passwords" on page 462

Checking out Account Passwords

When you add accounts for a domain to the Privileged Access Service, you store the passwords for those accounts securely in a local repository, in the Admin Portal, or in a key management appliance such as SafeNet KeySecure. If you have the appropriate global- or domain-specific permissions, you can check out the password for a stored account to access a domain computer. When you check out a password, you choose whether to display or copy it to the clipboard for use. The password remains checked out until either you check it back in or the Privileged Access Service checks it automatically.

The maximum length of time you are allowed to keep a password checked out is configured using a domain policy. For more information about configuring the Checkout lifetime policy for a domain, see "Setting Domain-specific Policies" on page 491

To check out a password:

1. In the Admin Portal, click **Resources > Domains** to display the list of domains.
2. Select a domain to display the domain details.
3. Click **Accounts**.
4. Select the appropriate domain account to display the Actions menu.
5. Select **Checkout** or **Request Checkout**.

   If you don't have the Checkout permission and click Request Checkout, your request is sent to a designated user or to the members of a designated role for approval. If your request is approved, you have limited period of time to check out the account password. For more information about the "request and approval" work flow, see [Managing Access Requests.]
6. Click **Show Password** if you want to view the password for the selected account as plain text or click **Copy Password** to copy the password without viewing it.

   The checkout is recorded as recent activity in the dashboard and in the list of domain activity.

7. Click **Close**.
8. Log on to the domain computer using the selected account name and password.

After taking the appropriate action, close the session to log off and check in the password. For more information about checking in a password, see "Checking in Passwords" on the previous page

Updating Domain Account Passwords

If you change the password for any stored account locally on a domain computer, the account password stored in the Privileged Access Service will no longer be valid. To synchronize the passwords so that the current password can be checked out and used to log on, you must update the password stored in the Privileged Access Service. You can update the password for managed or unmanaged accounts from the Accounts tab by selecting an account or by clicking **Accounts** when viewing the details for the domain.

When updating the password for an account, keep in mind that only characters that are standard ASCII characters are supported. Do not use a password that includes any extended ASCII or non-standard ASCII characters.

To update the password for a domain account:

1. In the Admin Portal, click **Resources**, then click **Domains** to display the list of domains.
2. Select the domain to display the domain details.
3. Click **Accounts**.
4. Select the account that no longer has a valid password stored in the Privileged Access Service.
5. Click the Actions menu, then select **Update Password**.

   The Update Password action is available for both managed and unmanaged accounts. In both cases, be sure you have the correct current password for the account. If you are unsure, reset the password on the domain computer first, then update the password stored in the Privileged Access Service.
6. Type the current password for the account you are updating.
7. Click **Save** to save the new password for the account.

Viewing all Domain Accounts

You can view the accounts that have been added for individual domains from the domain details. To see a list of all domain accounts for all domains, you can click the **Resources > Accounts** tab, then select **Domain Accounts**.

From the Domain Accounts list, you can search for domain accounts across all domains. You can also select an individual account for any domain to perform account-related actions—such as check out an account password or update the account's stored password. The information displayed on the Domain Accounts list is the same as the information displayed for accounts when you are viewing the details for a specific domain.

- **Logging on Without a Password**

  After you add account information to Privileged Access Service, other users with the appropriate global- or domain-specific permission can log on to domain computers using the account without knowing the password for the account.

  When you select an account stored in Privileged Access Service to log on to a domain computer, Privileged Access Service open a remote desktop connection on the target computer.

To log on using saved domain account information:

1. In the **Admin Portal> Resources** page, select the **Domains** tab.
2. Select a domain to display the domain details.
3. Click **Accounts**.
4. Select the appropriate domain account to display the Actions menu.
5. Select **Login** or **Request Login**.

   If you have the Login permission and the stored credentials are valid, clicking Login starts a new interactive secure shell or remote desktop session on the target resource. Within the secure shell or remote desktop session, most operations—such as cut and paste or resizing of windows—work as you would expect them to. For more information about working in the remote session, see "Deleting Domains" on page 671

   If you don't have the Login permission and click Request Login, your request is sent to a designated user or to the members of a designated role for approval. If your request is approved, you have limited period of time to start a new interactive secure shell or remote desktop session on the target resource.

Viewing Domain Activity

You can click Activity to review recent activity, such as password check out and check in activity, for the selected domain.

To view domain-specific activity:

1. Select the **Resources > Domains** tab.
2. Select the domain to display the domain details.
3. Click **Activity**.

Managing Secrets

Secrets are text strings or files that you want to protect. For example, you might have access keys, software licenses, or files that contain sensitive or confidential information to which you want to restrict access.

You can upload this type of information as raw text or in files up to a maximum of 5MB per file to store it securely. The information you choose to upload—whether it is a text string, a file, or a file and optional password—is encrypted before it is stored. After you upload files or text strings, you can use permissions to control which users are authorized to retrieve or replace the stored information when needed.

If you are a member of a role with a Privileged Access Service right or System Administrator right, you can view, add, modify, or delete secrets in the Secrets list or collections of secrets in folders or in the Sets list. If you are the owner of a text string or file because you uploaded it, you can grant permissions to other users, groups, and roles to work with the text strings and files you own.

In addition to creating and storing secrets, you can create folders to categorize and manage text and file secrets. Folders can be nested to create a folder hierarchy that makes it easier for you to organize your secrets. Folder permissions work similarly to the secret permissions and can be configured to allow access at various levels of the folder hierarchy.

Deleting Secrets or Folders

If you are the owner of a secret text string, stored file, or folder, you can delete any of the secrets or folders you own. If you are in a role with the appropriate administrative rights and have been granted the Delete and Retrieve Secret permission, or the secret is located in a folder that grants you the Delete and Retrieve Secret permission, you can delete the secrets and folders.

Note: You can delete a folder from the Admin Portal and the Privileged Access Service only if you have removed all secret files and subfolders from the folder.

To delete a secret or folder:

1. In the Admin Portal, click ***Resources***, then click **Secrets** to display the list of secrets.
2. Select the checkbox next to the secret or folder you want to delete.
3. Click the Actions menu, then click **Delete**.
4. Click **Yes** to confirm that you want to proceed with deleting the secret or folder.

Moving Secrets and Folders

You can change the organization of your folders and move secrets and folders to other folders. Folders and secrets can be moved up or laterally within the folder hierarchy. You cannot move a folder to one of its own subfolders. Once the folder or secret is moved, the path for the folder/secret is changed to reflect the new location. In order to move folders or files to a new location, you must have the **Edit** permission on the folder or file you want to move, and the **Add** permission for the destination folder. Also note the following:

- Moving a top-level folder also moves all the subfolder contents and members to the destination folder.
- Permissions and policies for a folder or secret being moved are inherited from the destination location, not from the source location.
- If you are moving a secret or folder, and there is already a secret/folder with the same name in the destination location, the move will fail.
- Moving a folder or secret to the top level of the Secrets page does not require the **Add** permission; only the **Edit** permission on the source folder or secret is required.

To move a folder location:

1. In the Admin Portal, click **Resources**, then click **Secrets** to display the list of folders and secrets.
2. Right-click on the folder you would like to move (to move a folder you must have the **Edit** permission).
3. Click **Move** from the drop-down menu.
4. Select the new folder location from the available options (only folders where you have **Add** permission are displayed).

Replacing Secrets

If you are the owner of a secret text string or stored file, you can edit the secrets you own. If you are in a role with the appropriate administrative rights and have been granted the Edit permission, or the secret is located in a folder that grants you the Edit permission, you can change the secret name, description, stored file, or password.

If you are updating a stored file with an optional password, you can choose to replace just the file, just the password, or both the file and password. For example, you might want to update the password associated with a file without changing the file you have stored. You should note, however, that the password stored with a secret file is not used to retrieve the file. They are simply stored together for convenience.

There are different ways to navigate to the Replace action. After you select this action, however, the steps are similar.

To replace a secret:

1. In the Admin Portal, click **Resources**, then click **Secrets** to display the list of secrets.
2. Select a secret to display its details.
3. Click the **Actions** menu, then click **Replace**.
   - If the secret is a text string, you can type or copy a new text string for the secret, then click **Save**.
   - If the secret is a stored file, you can set or change the password for the file, upload a different version of the same file, or browse to a completely different file to upload, then click **Save**.

   Note that you must click Save after making any changes for them to take effect.

Running Secret Reports

There are built-in Infrastructure reports that you can customize to view information about the secrets you have stored in the Privileged Access Service based on the criteria in which you are interested. For example, you can generate a report of the secrets that have been recently replaced. Similarly, you can generate a report that lists the secrets retrieved most often. You can then export the report to a file with comma-separated values or email the report to others.

To create reports about secrets stored in the Privileged Access Service:

1. In the Admin Portal, click **Reports**.
2. Click **Built-in Reports**, then click **Secrets** to display the list of reports available.
3. Select a report to display the results in a table.
4. Click **Actions** to copy the report, see or customize the report Details, Export the report to a file with comma-separated values, or Email the report to someone else or to a distribution list.

Searching the Secret List

You can search for specific secrets or folders using the search bar at the top of the Secrets page in the Admin Portal. You can search all objects in the entire list or only search for objects within a specific folder. When you search for items in a specific folder, the search function does not search for objects within a folders subfolders.

In addition to a full text search, you can also enter partial words in the **Search All Secrets and Folders** search field to isolate secrets or secret folders.

Note: Search functionality is case-sensitive.

To search for secrets or folders:

1. In the Admin Portal, click **Resources**, then click **Secrets** to display the list of secrets and folders.
2. Click the Secrets search bar.

3. Type the whole name or partial name of the secret or folder you are trying to locate.

   To narrow your search you can drill in to specific folders or subfolders.

Viewing and Changing Settings

You can view and change the secret or folder name and the optional description at any time after adding a text string or a file or a folder. You must have the **Edit** permission in order to change the settings.

To change secret settings:

1. In the Admin Portal, click **Resources**, then click **Secrets** to display the list of secrets and folders.
2. Select the secret or folder to display its details.
   - For Secrets, click the secret to display its details.
   - For Folders, click the check box next to the folder name, and then click **Edit** from the Actions menu.
3. Type a new name or a new description.

   If you are changing the folder name located within a folder hierarchy, you do not need to not enter the complete path; just the folder name.
4. Click **Save**.

Viewing Secret or Folder Activity

You can click Activity to review recent activity for a secret or secret folder. For example, if a stored file is downloaded, you can see when the activity took place and who downloaded the file.

To view activity for a secret or folder:

1. In the Admin Portal, click **Resources**, then click **Secrets** to display the list of secrets.
2. Select the secret or folder.
   - For Secrets, click the secret to display its details.
   - For Folders, click the check box next to the folder name and then click **Edit** from the Actions menu.
3. Click **Activity**.

Managing Services

Many organizations use domain or local accounts to run applications such as Windows services and Windows scheduled tasks or domain accounts used for IIS application pools on computers throughout the network. For security and auditing compliance, passwords for these types of accounts should be rotated periodically, but are

often left unmanaged because of the difficulty involved in updating passwords manually on multiple computers and the potential disruption of critical business services.

You can greatly improve security for the accounts used to run services by storing and managing these accounts and their passwords in the Privileged Access Service. After you identify the services that run using a local or domain service account you can automate password rotation without interrupting service availability.

In most cases, you add service and service account information to the Privileged Access Service by running discovery jobs that scan your network for information about computers in Active Directory domains. You can also manually add services and service accounts globally or on a system-specific basis.

Modifying Service Sets

After you have added a service set, you can modify the details about the set at any time. For example, you can add and remove members, change the set name or description, view recent activity, or update the permissions on the set.

However, you can't modify the membership type setting for existing sets. To change a set from manual membership definition to dynamic or from a dynamic query-based membership definition to manual definition, you must delete the existing set and create a new set.

To modify settings for a service set:

1. In the Admin Portal, click **Resources**, then click **Services** to display the list of services and scheduled tasks.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Change the set name, set description, or both, as needed.
4. If the membership definition is dynamic, you can modify the set membership by editing the **Query** field.
5. Click **Save**.

For more information about modifying other service set information, see the following topics:

- "Modifying Set Membership" on page 672
- Viewing Set Activity
- "Modifying Domain Sets" on page 672
- "Modifying Set Member Permissions" on page 672

Modifying Set Member Permissions

You can modify the permissions for the members of a set to control what other users can do on the service in the set. For example, you can assign member permissions to enable other users to view, edit, or delete the members of a set or to manage sessions on any member of the set. Member permissions are the same as the permissions you can assign to individual services or globally for all services. You can only assign member-level permissions on manual service sets, however.

For more information about the permissions you can assign to services, see "Setting Service-specific Permissions" on page 511

To assign member-level permissions:

1. In the Admin Portal, click **Resources**, then click **Services** to display the list of services and scheduled tasks.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Click **Member Permissions**.
4. Click **Add** to search for and select the users, groups, roles, or computers to which you want to grant set-specific permissions, then click **Add**.
5. Select the appropriate permissions for each user, group, role, or computer you have added.
6. Click **Save**.

Modifying Set Membership

For manual sets, you can modify the group membership directly from the system list by selecting the system, right-clicking, then selecting the Add to Set or Delete action. To change the set membership if members are defined using a SQL select statement, modify the query in the Settings for the system set.

Modifying Set Permissions

You can modify the permissions for a set to enable other users to view, edit, or delete the set or to grant permissions on the set to other users. You can assign permissions for the entire set on both manual and dynamic service sets.

The permissions assigned at the set level do not apply to the members of the set. For the members of dynamic sets, you can only assign member-level permissions through service-specific or global permissions. For manual service sets, however, you can assign member-level permissions for all members of the set.

To assign set-level permissions:

1. In the Admin Portal, click **Resources**, then click **Services** to display the list of services and scheduled tasks.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Click **Permissions**.
4. Click **Add** to search for and select the users, groups, roles, or computers to which you want to grant set-specific permissions, then click **Add**.
5. Select the appropriate permissions for each user, group, role, or computer you have added.
6. Click **Save**.

Modifying Service-specific Settings

After you discover or add services to the Privileged Access Service, you can change service-specific details, such as the service type, the service name, or the time restrictions for restarting the service after a password change.

In the most common scenario, you modify service-specific settings after running a discovery job to prepare for automated password management. For more information about updating a service after running a discovery job, see "Updating Service Settings" on page 613. For more information about preparing for password rotation, see "Automating Password Rotation" on page 507

Viewing a Service List

You can view the global list of discovered and manually added services by clicking **Resources**, then **Services** in the Admin Portal. You can also view the list of discovered services or manually added service information for specific

systems. Both the global and system-specific service list provide the following information:

- Name indicates the service name used to run the Windows service or the full path to the scheduled task.
- Description displays the display name associated with the Windows service or scheduled task.
- System indicates the target system where the service runs.
- Multiplexed account is empty until you configure automatic password management for the service. For example, this field is blank for newly-discovered services.
- Current account displays the local or domain account that the service is currently configured to run as.
- Type indicates whether the service is a Windows service or a scheduled task.
- Active indicates whether the Windows service or scheduled task with automatic password management is currently running on the system.
- Issues displays additional information about the status of the service. For example, if a service failed to restart or was not found on a target system, a message indicating the status is displayed.

Viewing Multiplexed Account Activity

You can click Activity to review recent activity for a multiplexed account. For example, if you have added a new multiplexed account or changed the sub-accounts associated with a multiplexed account, you can see details about the event.

To view account-specific activity:

1. In the Admin Portal, click **Resources**, then click **Accounts** to display the list of accounts.
2. Click **Multiplexed Accounts**.
3. Select the account to display the account-specific details.
4. Click **Activity**.

Viewing Multiplexed Account Status

After you create one or more multiplexed accounts, you can check the list of multiplexed accounts to see which sub-account had its updated most recently or if there were issues that prevented password rotation. For example, if you have changed one of the sub-accounts used to run a service, you might check the list of multiplexed accounts to see which sub-account is being used to run the service and whether any issues are reported.

To view the status of multiplexed accounts:

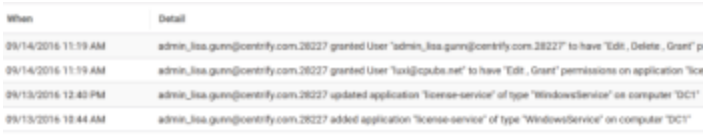
1. In the Admin Portal, click **Resources**, then click **Accounts** to display the list of accounts.
2. Click **Multiplexed Accounts**.
3. Check which sub-account displays the (Latest) label to indicate the most recent password change.
4. This is the sub-account currently being used to run the service.
5. Check whether the Issues column indicates problems finding the target, setting the credentials or accessing the service.

   The most common issues you might see are these:

- Failed to restart
- Failed to set credentials
- Service does not exist
- Administration credentials are not valid
- Cannot contact system

Viewing Service Activity

You can click Activity to review recent service activity, such as changes to the service settings or permissions, for the selected service. For example, if you have granted a new user access to the selected service or added a multiplexed account to a service, you might see information similar to the following:



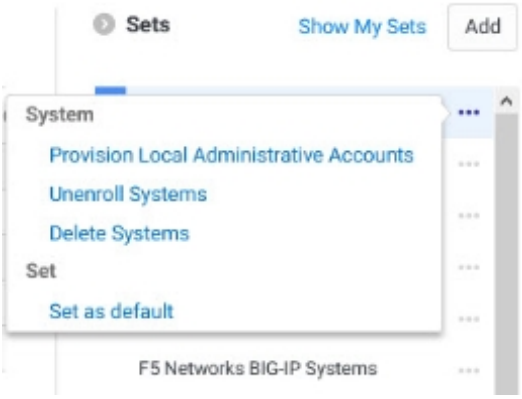
Managing Sets

You can manage different types of objects—such as applications, computers, network devices, domains, databases, secrets, services, and accounts—by organizing them into logical collections called **sets**. Organizing objects by using attributes they have in common simplifies management and reporting for the set members.

Most objects have predefined sets that you can use as filters. For example, there are predefined sets for local, domain, database, and multiplexed accounts. You can also create custom sets by manually adding and removing members or by defining queries. If you add a set, you can view and modify the set details and grant permissions to other users.

To perform a bulk action on systems for a set:

- Navigate to **Resources** > **Systems**.
- Select the dotted icon next to the set for the system bulk action.



- Select the action you want to perform for the systems within the set. The following bulk actions are available:

- Provision Local Administrative Accounts

  Note: This selection will immediately apply the action.

- Unenroll Systems
- Delete Systems

- In the confirmation window, confirm the action or close the window.

For more information about working with sets, see the following topics:

- "Adding System Sets" on page 536
- "Adding Domain Sets" on page 487
- "Adding Database Sets" on page 478
- "Adding Secret Sets" on page 502
- "Adding Service Sets" on page 506
- "Adding Account Sets" on page 475
- "Managing Application Sets" on page 830
- "Modifying Account Sets" on page 650
- "Rotating Credentials on Demand" on page 659

Identifying Default Sets

You can select any predefined or custom set to be used as the default set for new computers, network devices, domains, databases, services, or accounts. For example, you might want to use a custom query that places all computers on a specific subnet or that match a specific naming convention in the same set.

To identify a default set:

1. In the Admin Portal, click Resources, then click the section for the type of object for which you want to have a default set.
2. In the Sets section, right-click a set name, then click **Set as default**.

   Note that you can only have one default set for each type of object and that servers, workstations, network switches, and routers with local accounts are all **systems** objects. In addition to systems objects, there are object types for domains, databases, secrets, services, and accounts.

To change the default set, you can either right-click the set name, then click **Remove as default** or select a different set name, then click **Set as default** for that set.

Modifying Sets

After you have added a set for computers, network devices, domains, databases, secrets, services, or accounts, you can modify the details about the set at any time. For example, you can add and remove members, change the set name or description, view recent activity, or update the permissions on the set.

However, you can't modify the membership type setting for existing sets. To change a set from manual member definition to dynamic or from a dynamic query-based member definition to manual definition, you must delete the existing set and create a new set.

To modify settings for a database set:

1. In the Admin Portal, click **Resources**, then click the section for the type of object you want to change.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Change the set name, set description, or both, as needed.
4. If the membership definition is dynamic, you can modify the set membership by editing the **Query** field.
5. Click **Save**.

Viewing All Sets

If you're assigned to the system administrator role, you have the choice to view sets according to two different filters:

- Only the sets that you have been granted access to explicitly. For these sets, you or a role that you're assigned to has been granted access to view.
- All sets defined in the system, regardless of who created them.

By default, the sets you can see are the ones that you have explicit access to view.

For example, enabling this option can be useful in cases where a system administrator has left the organization but you still need access to the sets that they created.

> **Note:** If you have configured your deployment to automatically grant system administrators access to sets that other system administrators have created, those sets appear as part of the sets that you have explicit access to view or edit. For details about this setting, see "Viewing All System Admin Sets" below

To view all sets (System administrators only)

- When viewing any resource where there are user-created sets, click **Show All Sets** in the Sets area to the right to see all sets in the system, regardless of who created them.

  To see just the sets that you've created or sets that you have been granted explicit permission to, click **Show My Sets**.

  The link toggles between **Show All Sets** and **Show My Sets**, and the link appears for the view that you're not seeing currently.

Viewing All System Admin Sets

You can configure your deployment so that anyone assigned to the system administrator role can see new sets created by anyone in that role automatically. This way, all system administrators can view or edit sets created by other system administrators.

If system administrators have already created sets before you enable this setting, the setting affects only the sets that your administrators create *after* the setting is enabled. If you want your system administrators to access any sets that were created before you enabled the setting, you need to explicitly grant permission to those sets.

By default, this setting is not enabled.

To specify that all system administrators can access sets created by anyone in the system administrators role

- Go to **Settings** > **Resources** > **General** > **Security** settings, and enable the following setting:

  Automatically grant all set permissions to the system administrator role when a system administrator creates a new set.

Managing Systems

Individual systems—such as servers, workstations, switches and routers—are listed on the **Systems** page. You can populate this list automatically for some systems by running discovery jobs. Discovery enables you to create a profile to identify the systems in which you are interested—such as Windows or UNIX computers—then scan the network for systems that match the criteria you have specified. You can also add systems without running discovery jobs by adding individual systems manually or by importing multiple systems at once using an import file.

You can also manage systems by organizing them into groups. Organizing systems into logical **system sets** simplifies management and reporting for set members.

If you are a member of a role with the appropriate privilege management rights, you can view, add, modify, or delete individual systems in the **Systems** list or collections of member systems in the **Sets** list. If you are the owner of a system or a system set because you added it to the Privileged Access Service, you can grant permissions to other users, groups, and roles to work with the system or system set you own.

Changing System Settings

You can click System Settings to change the display name, DNS name, or IP address for any previously added system. You can also use the system settings to correct the system type, specify the protocol and port number for remote sessions, set a specific time zone for a system, and add or modify an optional description for the selected system. Other settings you can configure depend on the system type.

If you make changes to any of the system settings, click **Save**.

For more information about system-specific settings, click the following links:

- "Adding Windows Systems" on page 545
- "Adding UNIX Systems" on page 536
- "Adding Cisco IOS or NX-OS Systems" on page 524
- "Adding Cisco AsyncOS Systems" on page 523
- "Adding Juniper Systems" on page 531
- "Adding HP NonStop Systems" on page 528
- "Adding IBM i Systems" on page 529
- "Adding Check Point Gaia Systems" on page 521
- "Adding Palo Alto Networks PAN-OS Systems" on page 532
- "Adding F5 Networks BIG-IP Systems" on page 526
- "Adding VMware VMkernel Systems" on page 544
- "Adding Generic SSH Systems" on page 528

Deleting Systems

You can remove a system or systems from the Systems list and the Privileged Access Service.

1. In the **Admin Portal > Resources > Systems** to display the list of computers and network devices.
2. Select one system or multiple systems.
3. Click the **Actions** menu, then select **DeleteSystems**.
4. A **Bulk System Delete** dialog box appears where you can choose to save the password to secret. You will receive an email notification with details. That information is also available in **Job Reports**.

> **Note:** Bulk System Delete deletes all accounts for all selected systems, regardless if the account is active. To delete Sets, right-click on a set and select **Delete Systems** and go through the Bulk System Delete workflow.

Some things to remember with deleting passwords by bulk:

- Bulk System Delete only deletes accounts and systems you have permissions to delete.
- To retrieve the saved password secret, the secret file must be given "Retrieve" permission by a system administrator.

Deploying the user.ignore and group.ignore Configuration Files

You can deploy the user.ignore and group.ignore configuration files to one or more enrolled Linux systems. You can deploy these files to individual systems or all systems in a set, and to no more than 500 systems at a time.

If any of the selected systems are offline, the deployment won't work; you'll need to do the deployment again when those offline systems are back online.

The service stores the configuration files that you deploy, you can see a list of them at **Settings** > **Resources** > **Config Files**.

To deploy configuration files to Linux systems

1. In the Admin Portal, go to the **Systems** page select the desired systems:
   - For individual systems: select the desired Linux system(s), then click **Actions** > **Bulk Push Configuration File**.
   - For sets: select the desired set, click the drop-down menu (the ... button) and then click **Bulk Push Configuration File**

     The Bulk Push Configuration dialog box displays.
2. Enter the absolute path for the configuration file.

   For example:

   `/etc/centrifycc/user.ignore`

   `/etc/centrifycc/group.ignore`
3. Click **Browse** to navigate to and select the file you want to deploy.
4. Click **Submit** to deploy the file to the specified system(s).

If you're deploying to just one system, the service pushes the file to the system immediately. If you're pushing a file to multiple systems, the service adds the request to the job queue. When the job completes, the service emails you a report so that you can see which systems were updated and information about any deployment failures.

Modifying System-specific Details

When you are viewing the details for an individual system, you can also change system settings, view and add account information, define system-specific policies, review recent logon and password activity, and manage system-specific permissions. For more information about viewing and modifying system-specific information, see the following topics:

- "Changing System Settings" on page 687
- "Adding System Accounts" on page 534
- "Selecting Connectors" on page 499
- "Setting System-specific Policies" on page 556
- "Setting System-specific Advanced Options" on page 561
- "Viewing System Activity" on page 691
- "Setting System-Specific Permissions" on page 560
- "Setting Domain Operations for a System" on page 556

Removing System Account Info

You can remove an account for a system from the Privileged Access Service at any time. Removing a stored account from the Privileged Access Service does not affect account information stored locally on the target system. However, you must display or copy the password to the clipboard before the account can be deleted to help ensure you can continue to use the account with its correct password after removing it from the Privileged Access Service.

To remove an account from a system:

1. In the **Admin Portal > Resources > Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Click **Accounts**, then select the account you want to remove.
4. Open the Actions menu for the list of account, then click **Delete**.
5. Click **Show Password** if you want to view the password for the selected account as plain text or click **Copy Password** to copy the password without viewing it.
6. Record the password for future reference, then click **Close**.

Viewing Added Systems

You can click **Systems** in the **Resources** menu to display the list of servers and network devices and view the following information for all systems:

- Name is the unique name you use to identify the system.
- DNS Name/IP address is the fully-qualified domain name or IP address defined for the system in DNS.

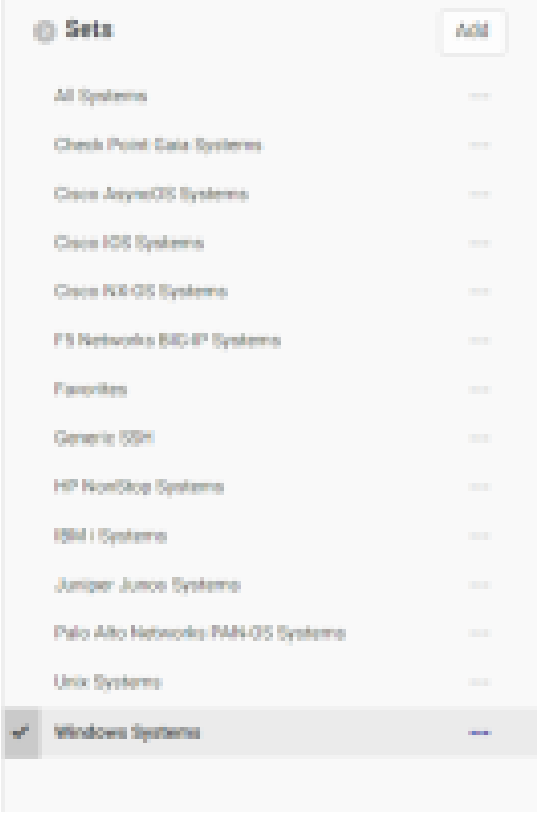
- Type specifies the type of system as a UNIX, Windows, Generic SSH, Cisco IOS, Cisco NX-OS, HP NonStop, Palo Alto Networks PAN-OS, IBM i, Check Point Gaia, F5 Networks BIG-IP, VMware VMkernel, Cisco AsyncOS, or Juniper Junos OS system.
- Last Test Result displays nothing if the last health check for the system was successful. A health check is performed when Test connection is selected from the Actions menu, when a system is added, and when a user logs on to a system using Privileged Access Service. If the system health check failed for any reason—for example, because the port used to check system health is blocked or a network connection to the system is not available—the column displays Unreachable or Unknown.
- Last Test displays the date and time of the last system health check. A health check is performed when Test connection is selected from the Actions menu, when a system is added, and when a user logs on to a system using Privileged Access Service.
- Discovered displays a time stamp, if the system was added during the discovery process. The time stamp indicates the time the system was added. If the system was added using a different method, such as manually or using the import process, nothing is displayed.

For more information about working with the Systems list, see the following topics:

- "Viewing Added Systems" on the previous page
- "Identifying Favorites" on page 458

Filtering Displayed Systems

By default, the Systems list displays all of the servers, workstations, and network devices you have added to the Privileged Access Service. You can filter the list by selecting a specific predefined or custom set. For example, if you only want to include Windows computers in the list, you can select the predefined **Windows Systems** set.



If you have added any manual or dynamic system sets, they are included in the list of available sets. You can then use those sets to select systems of a specific type or that match specific criteria, such as a custom query or the manual membership you have defined.

In addition to the predefined and custom sets, you can also filter the list of systems displayed by typing a search string, or by combining a filter and a search string. If you type a search string, systems and network devices with either a display name or a DNS name matching the string are included.

Identifying Favorites

As you add servers, workstations, and network devices to the system list, you might find it convenient to identify the ones you work with most frequently as favorites. You can identify the systems as your favorites by clicking the star icon next to the system name.

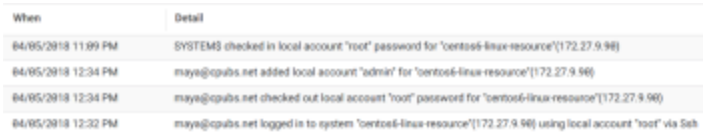
You can then filter the system list to only display the servers, workstations, and network devices that you work with most often. Identifying a system as a favorite also adds that system to the workspace you see when you click the Workspace tab, enabling you to see activity and take action at a glance without navigating the full list of systems that have been added to the Privileged Access Service.

Identifying a system as a favorite adds the system as an application tile in the Admin Portal on the Apps tab, allowing you to log on to the system manually directly from the Admin Portal.

Viewing System Activity

You can click Activity to review recent activity, such as password check out and check in activity, for the selected system. For example, if a user has successfully logged on to the selected system using a shared account, checked

out an account password, and had a failed logon attempt, you would see information about each of those successful and failed operations. The specific details listed for the system activity audit trail depend on the specific operations that have been most recently performed.



To view system-specific activity:

1. In the Admin Portal, click **Resources**, then click **Systems** to display the list of computers and network devices.
2. Select a system to display system-specific details.
3. Click **Activity**.

Viewing SSH Key Activity

You can click Activity to review recent activity for an SSH Key. For example, if an SSH Key is added, you can see when the activity took place and who added the key.

To view activity for a secret or folder:

1. In the Admin Portal, click **Resources**, then click **SSH Keys** to display the list of SSH keys.
2. Click a particular SSH key to display its details.
3. Click **Activity**.

Working with Resources and Remote Clients

You can add resources (systems, databases, domains, accounts, secrets, SSH keys, and services) to the Admin Portal and manage access to those resources.

For most systems that you add, you can log on and perform remote operations through secure shell (SSH) or remote desktop (RDP) sessions.

Change the RDP Certificate for Connectors

The NativeRDP functionality requires two files:

- A cert file `RDPServer.crt`
- A key file `RDPServer.key`

> **Note:** The RDP code does not produce, acquire, or generate these files. These files are obtained prior to starting NativeRDP, as a preliminary step performed by the connector and/or manual install.

This page explains how these files are found by the connectorand how to change the default behavior.

How Registry Keys Are Used

The Delinea Connector uses several registry keys to produce the RDP key files required for Native RDP functionality. These key/value pairs are located in `HKLM\SOFTWARE\Centrify\Cloud`.

Key	Type	Description
CPS.RDPHostThumbprint	String	A thumbprint for the certificate from the Windows Certificate Store. This is used to generate the key files.
Cps.RDPHostStore	String	The name of the Windows Certificate Store container. This is used to search for an installed certificate.This container name is relative to Cert:\LocalMachine\. The default name is Remote Desktop with the full path of CERT:\LocalMachine\Remote Desktop.
CPS.RDPHostCert	String	The encrypted content of the cert file.>**Note:** This is only for generated certificates.
CPS.RDPHostKey	String	The encrypted content of the key file.>**Note:** This is only for generated certificates.

How the Default Functionality Works

Generate Key Files from an Existing Certificate

By default, the Delinea Connector will attempt to generate the key files from an existing certificate . This certificate can be a self-signed certificate or one you've purchased (e.g. from GoDaddy), for use with NativeRDP.

Note: In order to locate the existing certificate, it **must** be installed in the Windows Certificate Store, under the LocalMachinecontainer.

By default, the connector will look for the file in Cert:\LocalMachine\Remote Desktop. This location can be changed using the CPS.RDPHostStore registry value. The connector looks in this store to find the thumbprint provided by the CPS.RDPHostThumbprint registry value. The thumbprint **must** be present to override the default behavior.

Generating a New Certificate If One Does Not Exist

If the connector does not find an existing certificate, it will generate one. When this happens, the connector wants to ensure the key files generated survive an upgrade, so they are backed up as secure registry values.

By default, a newly installed connector will generate its own certificate and back up the key files produced from that certificate in the secure registry keys CPS.RDPHostCert and CPS.RDPHostKey.

The certificate generated by the connector uses the default settings as defined by the N-Software third-party software library. See the "documentation for N-Software" for more information about the defaults used to generate the certificate.

The connector only sets the CN to the hostname, not the FQDNor IP.

Note: The auto-generated certificate has about a one year expiration and the certificate won't be auto-renewed.

If the certificate is expired, the user will see a prompt during the Native RDP connection about the certificate expiration.

Extracting Certificate Information

Once a certificate is present, the connector extracts the information into two files, `RDPServer.crt` and `RDPServer.key`. If these files were produced from a generated certificate, they also get backed up into secure registry values.

Once the backups exist, they are always used to restore the files on the disk when the connector starts. This means the following will occur:

- If you delete the key files from the disk, they will reappear "automatically".
- If the registry entries are removed, the connector will regenerate its own certificate for use.

To stop the default behavior, see Use your own certificate.

Using Your Own Certificate

To use your own certificate:

1. Get or create a certificate. The certificate must have an exportable private key. To generate a self-signed certificate that can be used with CentrifyNativeRDP:
   a. Ensure the following are met:
      - The certificate **must** be run on the connector machine.
      - The DnsName should be a comma delimited list of all names you want this cert to match against. Generally, it should be:
        - `FQDN` (For example, `hardhome.bespin.test`)
        - `Hostname` (For example, `hardhome`)
        - `IPAddress` (For example, `192.168.132.105`)
      - `FriendlyName` is optional, but recommended.
      - Set CertStoreLocation to the store name where this cert will be stored. This is always LocalMachine plus the directory name, for example RemoteDesktop. This value must match the value in the Delinea registry settings.

        Note: We recommend you use the default value for simplicity.

      - Set the `NotAfter` value, which supplies an expiration date. The example below uses a 3 year expiration from today.

   New self-signed certificate:

```
$SelfSignedCert = New-SelfSignedCertificate -Type SSLServerAuthentication -DnsName $name
-CertStoreLocation "cert:\LocalMachine\Remote Desktop" -KeyExportPolicy Exportable -
Provider "Microsoft Enhanced RSA and AES Cryptographic Provider" -NotAfter (Get-
Date).AddYears(3) -FriendlyName "Hello!"
```

2. Install the certificate in the Windows Certificate Store.

Get thumbprint:

```
PS> $SelfSignedCertificate.Thumbprint
PS> $SelfSignedCertificate.Thumbprint | clip
```

The installation:

- Displays the thumbprint.
- Copies the thumbprint to the clipboard for the configuration step.

3. Configure the connector to use the certificate:
   a. Update the registry on the connector machine.
   b. Create a string value for CPS.RDPHostThumbprint, and set it to the thumbprint copied from the previous step.

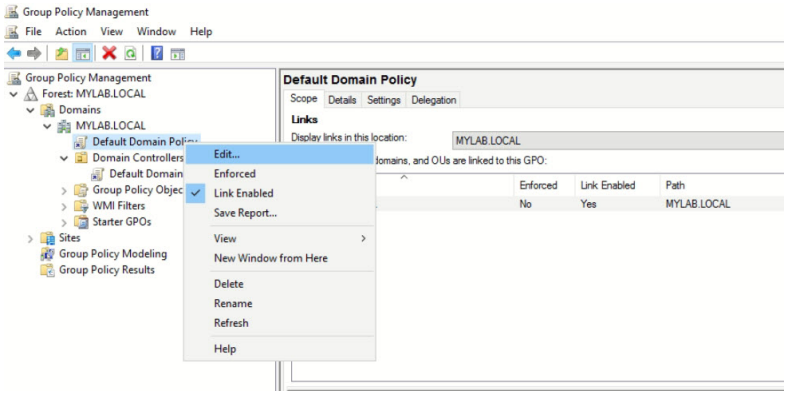
      Note: This is the key step in changing the default behavior.

   c. Restart the connector.
   d. (Optional) Delete the `CPS.RDPHostCert` and `CPS.RDPHostKey` registry values, if they exist.

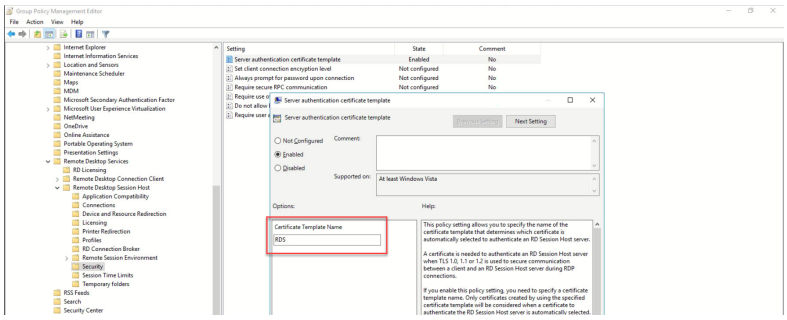
Replace a RDP Default Self-Signed Certificate

To replace a certificate which enforces with the default domain group policy:

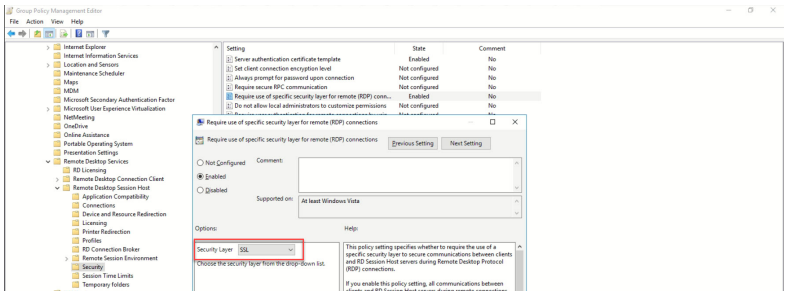
1. Open the Group Policy Management application and edit the **Default Domain Policy**. This applies the Certificate Template to all the servers in the AD Domain.



2. Navigate to `Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security`.
3. Open **Server Authentication Certificate Template** and for **Certificate Template Name**, enter the template name you created.



4. Navigate to `Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security`.
5. Open `Require use of specific security layer for remote (RDP) connections` and change the **Security Layer** to **SSL**.



6. Run gpupdate /force, and restart Remote Desktop Services to immediately apply the settings.

```
#Force GPO to update immediately
gpupdate /force#Restart RDS ServiceRestart-Service TermService
```

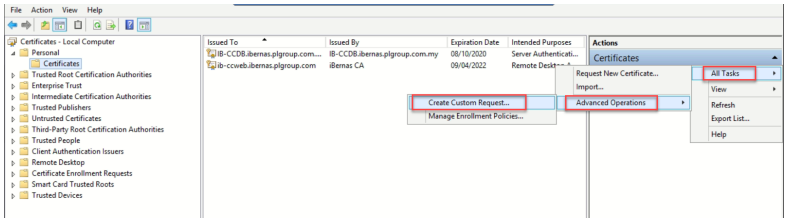
The RDS Authentication Certificate will be installed under Certificates (Local Computer).

To manually replace a RDP default self-signed certificate:

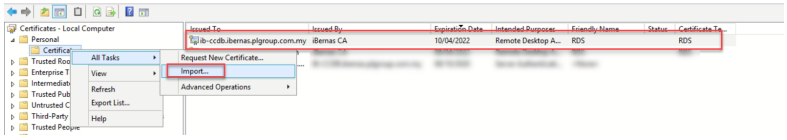
1. Open the Certificate Authority and modify the RDS template:
   a. On the **Compatibility** tab change the following:
      - **Certification Authority**: Windows Server 2008 R2 or above.
      - **Certificate recipient**: Windows 7 / Server 2008 R2 or above.
   b. On the **Subject Name** tab, select **Supply in the request** and the check **Use subject information from existing certificate for autoenrollment renewal request**.

To request a RDS Certificate from the server:

1. Open **Certificates - Local Computer** using `certlm.msc` and select **Create Custom Request**.



2. Set **Template** to **RDS** and click **Next**.
3. Click **Properties**.
4. For **Subject name**, set **Type** to **Common Name** and for **Type**, enter the server **FQDN** and click **Add**, then **Apply**.
5. On the **General** tab, specify a **Friendly name** to identify this certificate.
6. Choose the file path to save the offline request and click **Finish**.
7. Login to `http://CA_SERVER/certsrv` and click the **Request a certificate** link.
8. Click **advanced certificate request**.
9. Click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.**
10. Paste the content of the offline request into **Saved Request** and set **Certificate Template** to **RDS**.
11. Click **Download certificate**.
12. Import the certificate to **Certificates - Local Computer**.



13. Verify the thumbprint of the RDS Certificate:

```
Set-Location Cert:\LocalMachine\my
Get-ChildItemThumbprint                                    Subject----------
                              -------AA439E86EA877521C5A98460DBEBA70CC28C70E6  CN=ib-
ccdb.ibernas.plgroup.com.my
```

14. Replace the default self sign certificate with the RDS certificate:

```
#Replace Certificate for RDS
wmic /namespace:\\root\cimv2\TerminalServices PATH Win32_TSGeneralSetting Set
SSLCertificateSHA1Hash="AA439E86EA877521C5A98460DBEBA70CC28C70E6"
```

15. Verify the RDS Certificate installation:

```
Get-WmiObject "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices -Filter
"Termina
lName='RDP-tcp'"SecurityLayer                              :
2SSLCertificateSHA1Hash                  :
AA439E86EA877521C5A98460DBEBA70CC28C70E6SSLCertificateSHA1HashType             :
3Status                                  :TerminalName                          : RDP-
TcpTerminalProtocol                        : Microsoft RDP
8.0Transport                               : tcpUserAuthenticationRequired             :
1WindowsAuthentication                   : OPSComputerName                        : IB-
CCDB
```

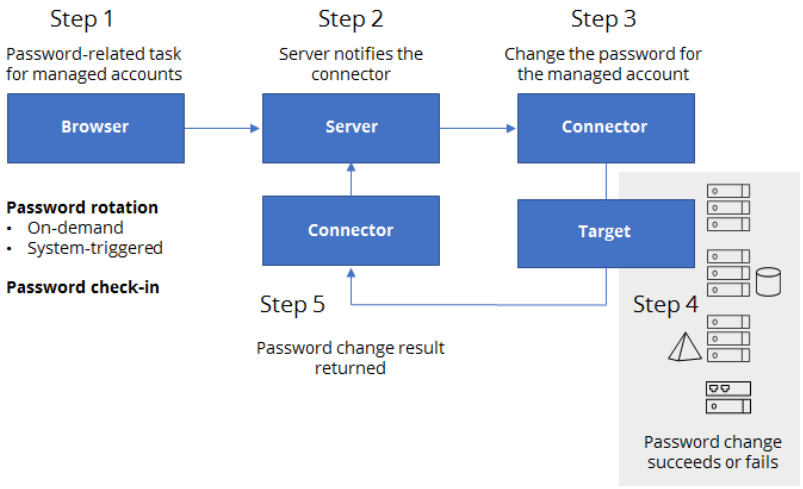
16. The new RDS Certificate will now connect to the server via Remote Desktop.

Communicating Password-related Activity

Most password-related operations are handled by background processes without opening an interactive secure shell or remote desktop session. However, the basic flow for password-related activity–such as automatic or on-demand password rotation and password updates when a password is checked in or when the maximum password checkout time has expired–is the same whether the operation is performed in the background or in a remote client session. The password-related operations are routed through the same architectural components of the infrastructure as logon operations. For technical reference, the following diagrams provide a simplified summary of the communication between components to complete password-related actions.

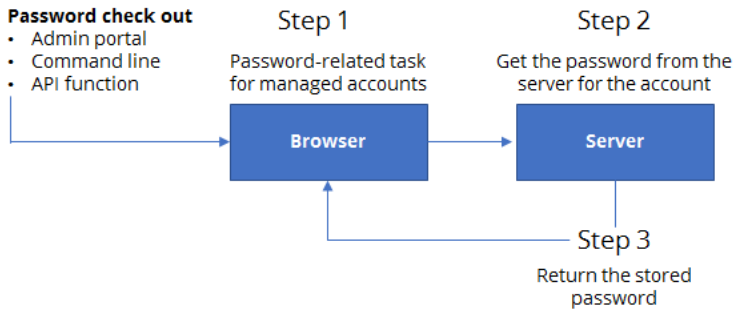
Password Rotation and Check in

The following diagram provides a simplified summary of the communication between components for scheduled or on-demand password rotation and checkin operations for managed accounts.



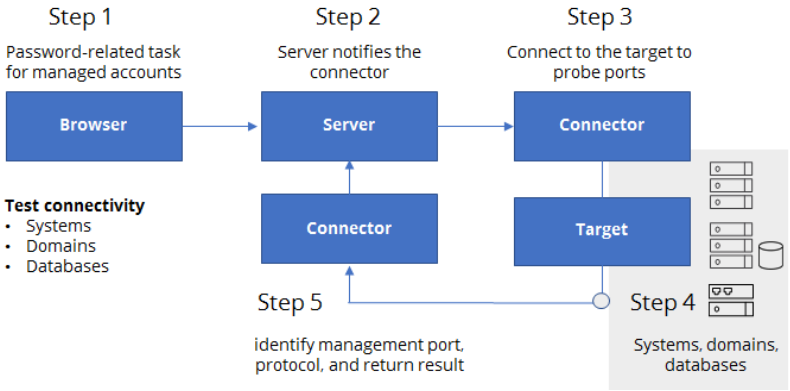
Password Checkouts

The following diagram provides a simplified summary of the communication between components for password checkout operations for managed accounts.



Network Access Verification

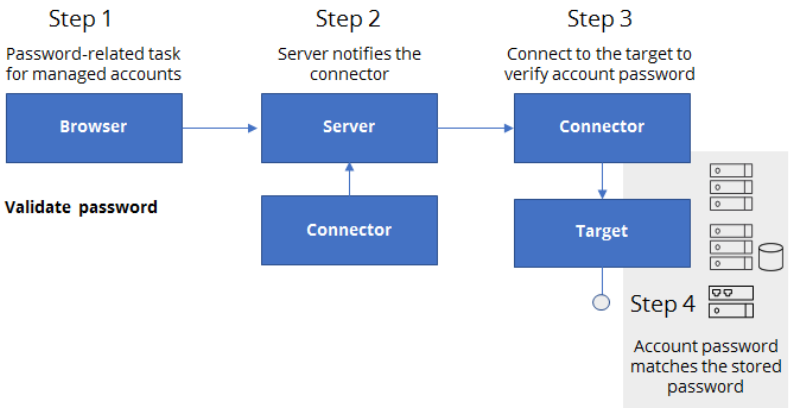
The following diagram provides a simplified summary of the communication between components for testing network access for systems, domains, and databases with managed accounts.



For Windows, the appropriate management port and protocol depend on the version of the operating system you are using and are detected by a port scan unless auto-detection is disabled. For more information about the management ports and protocols used for password-related operations, see "Managing Passwords for Local Accounts" on page 554

Password Validation

The following diagram provides a simplified summary of the communication between components for validating that the password stored for a managed account can be used to access the remote system.



For Windows, the appropriate management port and protocol depend on the version of the operating system you are using and are detected by a port scan unless auto-detection is disabled. For more information about the management ports and protocols used for password-related operations, see "Managing Passwords for Local Accounts" on page 554

Configuring Remote Clients

You must have the RDP or SSH gateway service enabled for at least one connector to log on remotely to target systems using a remote client program. If the gateway service is available for a connector in your infrastructure and you have appropriate View and Login permissions, you can log on either by using stored account information or by manually specifying a user name and password.

By default, remote client connections use a web-based browser client. You can also configure remote connections to use a local Windows client or native UNIX SSH or RDP client instead of the default web-based client. Regardless of the client program you use, however, the connections to target systems require the RDP or SSH gateway service to be enabled on an available connector and internal or external network access to the target system.

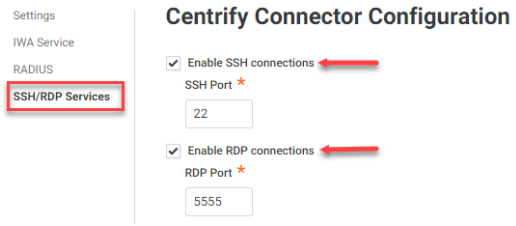
Selecting Connector Services

Before you can use a secure shell session (SSH) or remote desktop protocol (RDP) session to connect to target computers, you must configure one or more connectors to act as the SSH service or RDP service gateway. The SSH/RDP service gateway enables you to control network traffic through the connector to target computers to support a separation of duties security model.

Note: RDP connections require that the Delinea Connector be version 18.5 or newer.

To configure a connector to act as a SSH/RDP service gateway:

1. In the Admin Portal, click **Settings**, then click **Network** to display Delinea Connector settings.
2. Select a connector to display the Actions menu.
3. Select **Modify** from the Actions menu, then click **SSH/RDP Services**.
4. Click **Enable SSH connections** and/or **Enable RDP connections** and specify the ports if you are not using the default ports.



If you are configuring a connector version 18.4 or older, the RDP configuration options are not available.

5. Click **Save**.

For more information about modifying other connector settings, see the connector-related topics in the Admin Portal help.

If you enable the RDP or SSH gateway for a connector, remote sessions display a default welcome message to authorized users when they log on using the default web-based browser client, local Windows-based client, or a native RDP or SSH client. For information about defining a custom banner or restoring the default gateway banner, see "Updating the SSH Gateway Banner" on page 753

Selecting Remote Clients

For most systems that you add to the Privileged Access Service, you can log on and perform remote operations through secure shell (SSH) or remote desktop (RDP) sessions. There are different client options available for connecting to a target system. The options available depend on the operating system of the target computer, the clients supported by the operating system you are using to connect to the target computer, and your user preferences.

You can access remote systems in the following ways:

- Using the default web-based client to remote access a system.
- Using Direct RDP or SSH to access a remote system.
- Using a native Windows client with the Remote Access Kit.

Accessing Remote Systems

By default, if you have the View and Login permissions, you can log on to remote systems from the Admin Portal using the default web browser-based client. You can also configure remote sessions to start by launching a local Windows client with an appropriate command or a direct RDP or SSH configuration file. Both of these options enable you to log on to the target system from the Admin Portal through the Delinea Connector.

Logging on to a target system through the connector has several advantages. For example:

- You can watch and terminate remote sessions.
- You can view session activity in the portal and in reports.
- You can configure authentication rules and authentication profiles for remote access.
- You can capture and playback audited remote activity.

Privileged Access Service allows you to access remote systems in the following ways:

- Using the web to remote access a system.
- Using a native Windows client with the Remote Access Kit.
- Using Direct RDP or native SSH to access a remote system

Procedures

Using the Web to Remote Access a System

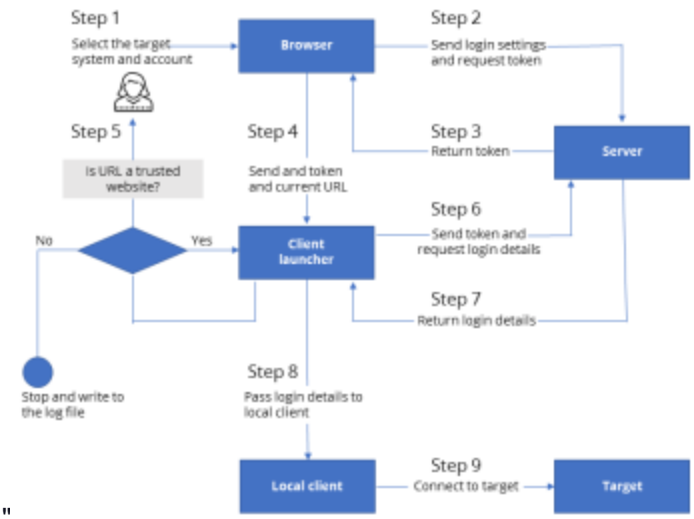
To use the default web browser-based client to remote access a system, see "Using Default Web-based Clients" on page 711

Using a Native Windows Client with the Remote Access Kit

As an alternative to using the default web-based client, you can configure remote connections to use a **local Windows-based client** or **native UNIX client**. By configuring remote connections to use a local Windows-based client or a native client, you can use a familiar interface you are comfortable with for performing remote operations. However, these clients and remote connections still require you to enable the SSH or RDP gateway service for at least one connector before you can log on remotely to target systems using secure shell or remote desktop sessions. If the gateway service is available for a connector in your infrastructure and you have appropriate permissions, you can log on either by using stored account information or by manually specifying a user name and password. For information about how to configure a local Windows-based client instead of the default web-based browser for remote connections, see "Selecting User Preferences" on page 764. For information about how to use a native UNIX client for remote connections, see [Using Direct RDP or Native SSH to Access a Remote System.] For information about adding the gateway service to a connector, see "Selecting Connector Services" on page 700

If you decide to use a local Windows-based client for remote connections, you have the option to download and install a separate "client launcher" application that is part of the Remote Access Kit software package. The Remote Access Kit enables you to execute the command to open the local client and pass arguments to it without manually typing the command and its arguments every time you open a new session. If you download the Remote Access Kit and trust the website detected for the current cloud server, Privileged Access Service adds the host name for the current cloud server to a list of trusted websites for launching the local client. This information is stored the `HostWhiteList` registry key on the computer that hosts the local Windows-based client. You can add other host names to the list of trusted websites or remove host names from the list to ensure the arguments used to invoke the local client are only passed from the secure websites that you trust.

The following diagram illustrates the basic flow when you use a local Windows-based client with the client launcher.



As illustrated in the diagram, selecting a target and account for remote access in the Admin Portal sends initial login information and the request for a token to the server that handles process requests (REST call: GetAuthToken). The server returns the authentication token, which is cached by the Admin Portal, and sent with the login information and current URL to the client launcher. The client launcher checks the `\HKEY_CURRENT_USER\Software\Centrify\CpsRun\HostWhiteList` registry key to determine whether the URL is listed as a trusted website. If the URL isn't listed but the user specifies it is a trusted website, the client launcher requests additional login details (REST call: GetLoginDetails) from the server and passes the login details to a local client—such as PuTTY or a remote Session Host—to connect to the target system.

You can remove a trusted website for the client launcher by manually editing the registry entry on the computer that hosts the local client. If you attempt to add a trusted website and don't see confirmation that the operation was successful, it might indicate that there is a security issue, such as invalid or expired credentials. For more information about specifying URLs for trusted websites and the success or failure of the operation, see the client launcher log file. By default, the log file `log.txt` is found in the `Program Data\Centrfy\CPS Run Log` folder.

Note: Keep in mind that manually editing the registry can result in making a system unstable or unusable if not done properly, Only experienced administrators should modify registry keys directly.

Changing Windows-Based Client Session Display Size

You can set a user preference to specify the default window size for remote sessions to adjust to different display requirements. For example, if you are viewing sessions using a tablet or a computer with a small monitor you might want to change the display size to suit a smaller screen than when you are working with a full-scale desktop monitor.

If you have administrative rights for the Privileged Access Service, you can change the window size for remote sessions from the Admin Portal by setting a user preference.

For more information about changing the window size for Windows-based client sessions, see "Selecting User Preferences" on page 764

Downloading and Testing the Remote Access Kit

If you want to use the local Windows-based client for remote sessions, you can download and install the **Remote Access Kit** for Windows computers. After you have downloaded and installed the software package or if you need to verify access to it on a specific local computer, you can test for the availability of the program before you attempt to open sessions using the local Windows-based client.

if you have administrative rights for the Privileged Access Service, you can download, install, and test access to the remote access kit from the Admin Portal by setting a user preference.

For more information about changing the window size for Windows-based client sessions, see "Selecting User Preferences" on page 764

Downloading and Installing the Remote Access Kit

1. In the Admin Portal, click **Settings**, then click **Resources** to display the settings available for the Infrastructure Services.
2. Click **User Preferences**.
3. Select the local Windows-based client to use for SSH and RDP sessions.
4. Click **Download** to download the Remote Access Kit software package that contains the local client launcher.
5. Open the downloaded file and follow the prompts displayed to install the software.
6. Click **Save**.
7. Downloading the installing the Remote Access Kit automatically downloads the RDP file for launching a Windows Remote Desktop Connection.
8. If you want to immediately verify installation on the local computer, select **I have installed the Remote Access Kit on this computer** then click **Test**.
9. Click **Open Delinea Remote Access Kit** to complete verification.
10. If you trust the website URL for the current cloud server, click **Yes**.

If you do not download and install the Remote Access Kit on the local computer, review the instructions displayed for information about how to start sessions using the local Windows-based client with command-line arguments.

Testing the Availability of the Remote Access Kit

1. In the Admin Portal, click **Settings**, then click **Resources** to display the settings available for the Infrastructure Services.
2. Click **User Preferences**.
3. Select **I have installed the Remote Access Kit on this computer**.
4. Click **Test**.
5. If you have installed the Remote Access Kit on the local computer, you are prompted to open it.
6. Click **Open Delinea Remote Access Kit** to complete verification.
7. If you trust the website URL for the current cloud server, click **Yes**.

If you do not download and install the Remote Access Kit on the local computer, review the instructions displayed for information about how to start sessions using the local Windows-based client with command-line arguments.

Accessing Remote Systems with Direct RDP or Native SSH

In some cases, you might want to log on remotely to a target system using a stored account, but without using the portal at all. You can do so by specifying the connector host name or IP address. You use a cloud user's username to begin the session along with the connector IP/FQDN and port. The connector port is the port specified in the connector settings.

The connection client will then prompt you for all the information needed to authenticate your identity and access the target system. For example, if you have not preconfigured any connection strings, you might need to provide your user name and password, a second form of authentication if you have a profile that requires multi-factor authentication, the host name or IP address of the target system, and the stored account you want to use to log on to the target system.

Opening the connection might look similar to the following:

```
login as: joey@acme.net
Password: ********
Answer security question 'Favorite clown': ******
Hostname: win1.acme.net
Account: qadmin
```

Connection Strings

The username is critical when using Direct RDP or SSH to access a system. You need one of the following connection strings to log into a remote system:

- localaccount@systemname@clouduser.
- systemname@clouduser.
- clouduser.

Note: For SSH, you can use your own connection strings. Additionally, with SSH you can use browserless or direct file transfer.

Direct RDP or SSH Clients for Connecting to Remote Systems

Delinea PAS supports any clients that support RDP files including Microsoft Remote Desktop.

Logging into a Remote System using Direct RDP or Native SSH

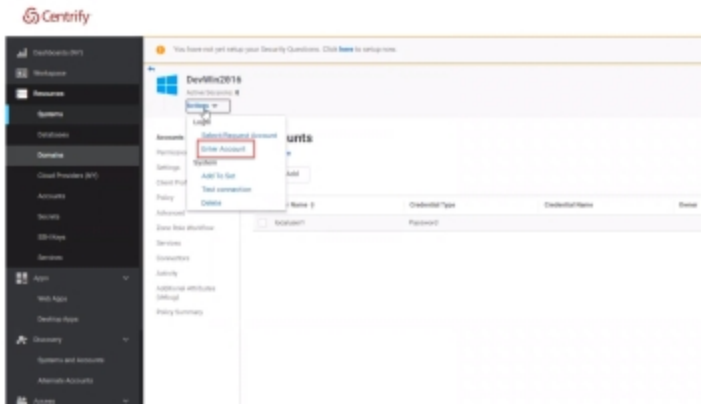
You can use native clients such as MSTSC or Putty to directly log into a remote system.

Note: Users with more than 500 sets and/or collections should expect some latency until the connection to the target is made. As such, providing the whole connection string (example: account@system@clouduser) may reduce this time by a few seconds.

To use Direct RDP or SSH to log into a remote system

1. Open a Direct RDP or SSH session.
2. On the **General** tab, for **Computer** , enter the connector IP or FQDN and the port. And for the user name, you use a "connection string."
3. Click **Connect**.
4. A command window appears and you will then be asked to enter a password for the account you are trying to access followed by a host name.
5. Next, you can choose a vaulted user or local user. If you choose a vaulted account, you will proceed with entering the account name. If you enter an account that is not vaulted, you will be prompted to manually log into the system:

In the Admin Portal, the same operation is done by navigating to the Admin Portal **Systems** > select and account > **Accounts** > **Actions** > **Enter Account**:



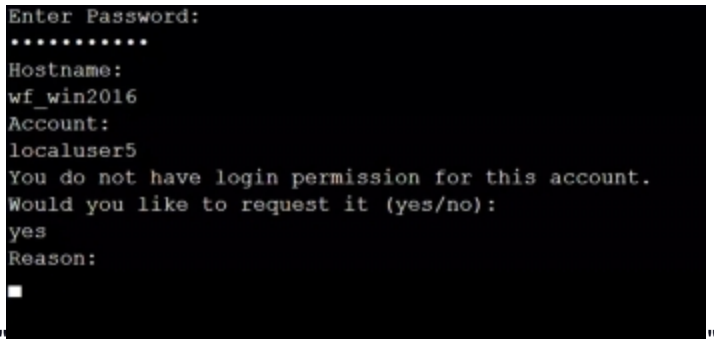
whereby you will be asked to manually enter the user name and password.

1. Enter the user name and password and click **Login**.

Logging in with a Workflow-enabled Account

If Workflow is enabled, direct RDP/SSH using this account submits a request for login permission. From your RDP or SSH, attempt to access an account. You will be asked to request login permission for an account, similar to the

following:



Once the workflow request is submitted, much like all Delinea workflow, you will be emailed and have a request waiting for you in Delinea PAS (**Access** > **Requests**) and can approve or reject. Once the workflow is approved, you can login. If the workflow is rejected, you will be asked to request login permission again. For additional information on Workflow for accounts, see "Configuring Global Account Workflow" on page 758

Logging in with a Non-PAS-Vaulted Account (manual login)

If an account is not vaulted, direct RDP/SSH using this account to manually login. From the RDP or SSH client, access an account that is not vaulted using the account name for the user name. You will be asked if you want to log in manually and you proceed to log in manually. For more information on manually logging into a system, see "Manual Logon" on page 472

Logging in with an MFA-Enabled Account

If MFA is enabled, direct RDP/SSH using this account challenges the user with the challenges defined on the profile. From the RDP or SSH client, enter the password and for **Hostname**, enter the IP address or the system name. You then choose a system and will be asked if you wish to manually login and you manually log in and answer any MFA questions set up on the account. For more information on authentication rules, see "Creating Authentication Rules" on page 281

Logging in with a Reconciliation-Enabled Account

If an account is reconciliation-enabled, direct RDP/SSH using this account resets the password and reconciles it. From the RDP or SSH client, you can log into a faulty account and the password is corrected. Faulty accounts are only corrected if reconciliation is enabled. If not, login will fail. For more information on password reconciliation, see "Configuring Domains for Local Account Password Reconciliation" on page 549

Logging in with a Discovered Missing-Password Account

If an account is discovered and missing a password, direct RDP/SSH using this account changes the account and grants access to the system. From the RDP or SSH client, you can log into an account using manual login for discovered accounts that do not have passwords. For more information on discovering accounts, see "Assigning Alternative Account Profile Management Permissions" on page 584

Viewing Reports for Remotely Accessed Accounts

There are two reports that provide information on remote accessed accounts. You can access them from the Admin Portal> **Reports**:

- Remote Sessions Activity: displays information on any RDP/SSH session from a specific date.
- Remote Sessions Count: displays number of RDP/SSH sessions by connector type.

For more information about accessing remote systems, see the subtopics to this page.

Additional File Operations

Overview

In a similar way, you can also perform secure copy (scp), and secure file transfer (sftp) operations using a native client. By accessing files on a target computer through the Delinea Connector, you can authenticate with your own credentials, then use the local or domain accounts stored in the Privileged Access Service to perform secure file operations on a remote computer. No direct interaction with the portal is required, but the activity is captured and visible in dashboards and reports.

As with secure shell sessions, you can log on manually without using a stored password if you have a user name and password with File Transfer permission. If you don't have the File Transfer permission, you can request access from a designated approver if a request and approval work flow is enabled.

The information you provide to authenticate and access the target computer is the same as the information required to open a secure shell session. However, you must have the File Transfer permission to perform scp or sftp operations.

For example, to copy a file from one computer to another using scp, the connection information would be similar to the following:

```
/home/smith02$ scp Login-user@Connector-FQDN:Source-filenameDestination-filename
```

You would then be prompted for the login-user password, the target computer host name, and the target account and use sftp command to perform operations.

You can perform many additional file operations using the secure file transfer protocol. For example, you can use sftp to list directory contents, rename files, or delete files. The connection information would be similar to the following:

```
/home/smith02$ sftp Login-user@Connector-FQDN
```

You would then be prompted for the login-user password, the target computer host name, and the target account.

The scp and sftp file transfer protocols are supported for any target system type and most native clients regardless of the operating system from which the connection is made.

Interactive Authentication

On some platforms, the sftp client cannot perform interactive authentication when multiple prompts are required. If the sftp client can't communicate with the connector for authentication, you can use a connection string profile to specify the parameters required to complete the file transfer.

Connection Strings

In addition to the formats described in "Saving connection profiles", a new field may be prepended to the connection string to indicate whether you need shell access or file access. Adding the type of access to the connection string is useful in scripts to skip the following interactive prompt:

```
Do you need ssh shell access or file transfer access?
```

For domain accounts, the format is:

```
accesstype@domainUser@domainName@hostname@user
```

For local accounts, omit the **domainName**, as in:

```
accesstype@localUser@@hostname@user
```

SSH connection strings

You can use an SSH client connection string to connect.

`ssh user@targetHostname@loginAccount@connectorHostname`

The connection string consists of:

- User: Local account of the target machine (**user@targetHostname**)
- Delinea PAS Cloud username (**loginAccount**)
- Connector hostname: (**connectorHostname**)

> **Note:** If the target hostname or account isn't specified, you will be prompted for this information.

For example:

`ssh myuser@111.111.111.111@pascloudeuser@email.com@222.222.222.22`

This will generate a password prompt and any other required authentication prompts.

Authenticating to PAS

The login user name and password is the same information you would use to log on to the portal. For example, the login user could be a Delinea Directory user or an Active Directory user.

If you have any login authentication profiles that require multi-factor authentication, you might be prompted to select a mechanism or respond to a challenge.

Saving Connection Profiles

Most secure shell clients allow you to save the connection string profiles you use to enable you to log on with minimal interactive input. For example, you might want to save your login user name and the connector host name you use most frequently in a profile to reduce the information you need to provide to log on to different target systems.

The connection string can include the following fields:

```
user
hostname@user
account@hostname@user
```

The **user** field specifies the identity service user name you would use to log on to the Admin Portal.

The **hostname** field is the DNS host name of the system you added to the Privileged Access Service. If you have access to more than one system with the same DNS host name, you are prompted to select which system to use.

The **account** field is the account you want to use to log on to the target system. If the account field contains the @ character, it is assumed to be a domain account. Otherwise, it is assumed to be a local account.

A simple connection string might include all three fields. For example:

`root2@suse.demo.net@gunro12@demo.net`

You can also omit fields in the connection string. You will then be prompted for any omitted fields. For example, in the following connection string, local1 is the account used to log on to the target system, the DNS name of the target system is omitted, and the identity service user name is `richcis@richl.devp`.

```
local1@@richcis@richl.devp
```

Specifying the Account

You can specify any account you want to use to log on to the target system. The account can be a domain account or a local account. In most cases, the account is a privileged account with a managed password, but it is not required to be.

- If you have **View** and **Login** permissions on the account, the connection is established and you have access to the target system.
- If you have **View** permission on the account, but do not have the Login permission, you are prompted for whether you would like to request access to the account. If you request access, you are prompted for a reason and the request is submitted to a designated approver, and the current session is closed.
- If your request is approved, you could reopen the native secure shell client and log on to the target system successfully.

- If you are prompted to request access and choose No, you can continue logging on to the target system but you must know the password for the account.
- If you don't have **View** permission for the account you specify or the account isn't an account stored in the identity service, the target system will prompt you to provide the password for the account and a second form of authentication if multi-factor authentication is required for the account.

Specifying the Target System

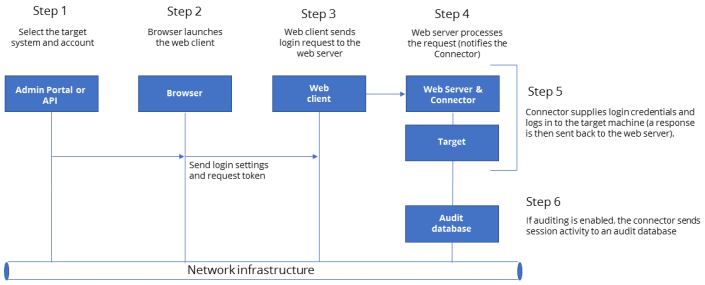
After successful authentication for the identity service, you can specify the host name or IP address for the target system. If the DNS name is stored for the target, you must specify the fully-qualified domain name. If the IP address is stored for the target, you must specify the IP address. There is no automatic translation between IP addresses and host names.

If the target is found and logging on requires multi-factor authentication, you might be prompted to select a mechanism or respond to a challenge.

Using Default Web-based Clients

The default web-based browser client simulates a native secure shell or remote desktop connections that you can open from within the Admin Portal.

The following diagram illustrates the basic flow of operation for logging on using the default web browser client.



The network infrastructure might be internet connectivity for access to Delinea-managed tenants, an internal corporate network inside or outside of a firewall, or a private or public cloud instance that you manage for your organization.

Operationally, using the default web-based browser client is similar to using any other SSH or RDP program. Most features work as you would expect.

Working with SSH Sessions

Logging on to a target Linux or UNIX server or to a network device that supports SSH opens a new web-based SSH session terminal. You can then resize the session window by dragging its borders, maximize or minimize the display area while the session is open, or close the window to end the session. You must use a mouse to copy and paste in the secure shell, however, because Ctrl-C is used to terminate operations in UNIX-based environments.

Working with RDP Sessions

Logging on to a target Windows system opens a new web-based RDP connection. You then can resize the window by dragging its borders, maximize or minimize the display area while the session is open, or close the window to end the session.

Menus and keyboard shortcuts operate in the same way as when you log on locally to a Windows computer.

However, there are some features that you might not be able to use when you access a target system with a remote desktop session and the default web-based browser RDP client. For example, the following features are not supported:

- Printer redirects
- Audio
- Drive redirects
- COM port redirects

Changing Display Size for Web-based Client Sessions

You can set a user preference to specify the default window size for remote sessions to adjust to different display requirements. For example, if you are viewing sessions using a tablet or a computer with a small monitor you might want to change the display size to suit a smaller screen than when you are working with a full-scale desktop monitor.

If you have administrative rights for the Privileged Access Service, you can change the window size for remote sessions from the Admin Portal by setting a user preference.

For more information about changing the window size for web-based client sessions, see "Selecting User Preferences" on page 764

Web-based RDP-Browser-Client Keyboard Shortcuts

The following table shows the web-based RDP browser client/desktop app keyboard shortcuts and how they correspond to standard Windows keyboard shortcuts. They also apply to Windows desktop applications launched via Admin Portal.

Shortcut for Web-based RDP browser clients/desktop apps:	Functions similar to Windows Shortcut:	Function:
Alt-PgUp	Alt-Tab	Allows you to switch between applications (left to right).
Alt-PgDn	Alt-Shift-Tab	Allows you to switch between applications (right to left).
Alt-Home	Ctrl-Esc	Displays the Start menu.
Alt-Delete	Alt-Space	Displays the Windows menu.

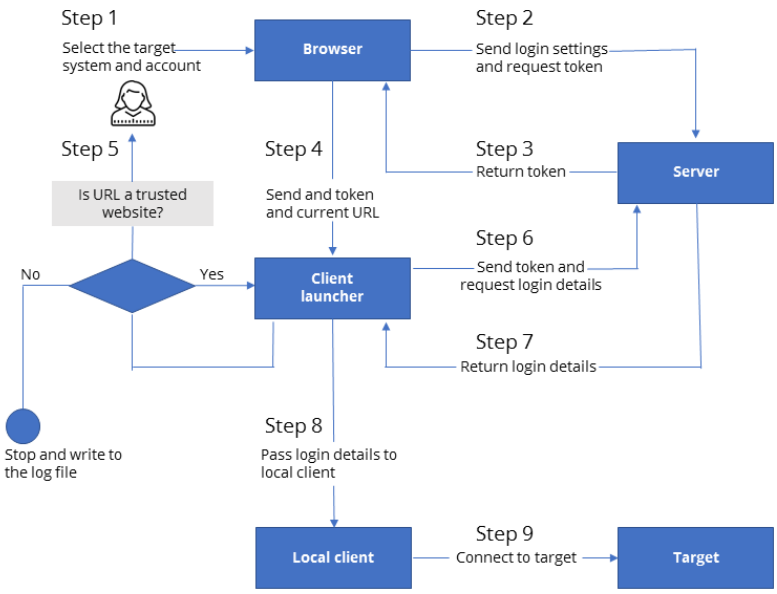
Shortcut for Web-based RDP browser clients/desktop apps:	Functions similar to Windows Shortcut:	Function:
Ctrl-Alt-NumKey minus (-)	Prtsc	Allows you to take a screenshot of the entire desktop.
Ctrl-Alt-NumKey plus (+)	Alt-Prtsc	Allows you to take a screenshot of the active application.
Alt-Insert	Alt-Esc	Allows you to cycle through the open applications in the order they were launched.
Ctrl-Alt-End	Ctrl-Alt-Delete	Displays the Windows Security dialog box.
Alt-Shift-Home	Ctrl-Shift-Esc	Starts the Windows Task Manager.

Using Local Windows-based Clients

As an alternative to using the default web-based client, you can configure remote connections to use a **local Windows-based client** or **native UNIX client**. By configuring remote connections to use a local Windows-based client or a native client, you can use a familiar interface you are comfortable with for performing remote operations. However, these clients and remote connections still require you to enable the SSH or RDP gateway service for at least one connector before you can log on remotely to target systems using secure shell or remote desktop sessions. If the gateway service is available for a connector in your infrastructure and you have appropriate permissions, you can log on either by using stored account information or by manually specifying a user name and password. For information about how to configure a local Windows-based client instead of the default web-based browser for remote connections, see "Selecting User Preferences" on page 764 For information about how to use a native UNIX client for remote connections, see "Accessing remote systems." For information about adding the gateway service to a connector, see "Selecting Connector Services" on page 700

If you decide to use a local Windows-based client for remote connections, you have the option to download and install a separate "client launcher" application that is part of the Remote Access Kit software package. The Remote Access Kit enables you to execute the command to open the local client and pass arguments to it without manually typing the command and its arguments every time you open a new session. If you download the Remote Access Kit and trust the website detected for the current cloud server, Privileged Access Service adds the host name for the current cloud server to a list of trusted websites for launching the local client. This information is stored the `HostWhiteList` registry key on the computer that hosts the local Windows-based client. You can add other host names to the list of trusted websites or remove host names from the list to ensure the arguments used to invoke the local client are only passed from the secure websites that you trust.

The following diagram illustrates the basic flow when you use a local Windows-based client with the client launcher.



As illustrated in the diagram, selecting a target and account for remote access in the Admin Portal sends initial login information and the request for a token to the server that handles process requests (REST call: GetAuthToken). The server returns the authentication token, which is cached by the Admin Portal, and sent with the login information and current URL to the client launcher. The client launcher checks the `\HKEY_CURRENT_USER\Software\Centrify\CpsRun\HostWhiteList` registry key to determine whether the URL is listed as a trusted website. If the URL isn't listed but the user specifies it is a trusted website, the client launcher requests additional login details (REST call: GetLoginDetails) from the server and passes the login details to a local client–such as PuTTY or a remote Session Host–to connect to the target system.

You can remove a trusted website for the client launcher by manually editing the registry entry on the computer that hosts the local client. If you attempt to add a trusted website and don't see confirmation that the operation was successful, it might indicate that there is a security issue, such as invalid or expired credentials. For more information about specifying URLs for trusted websites and the success or failure of the operation, see the client launcher log file. By default, the log file `log.txt` is found in the `Program Data\Centrfy\CPS Run Log` folder.

Note: Keep in mind that manually editing the registry can result in making a system unstable or unusable if not done properly, Only experienced administrators should modify registry keys directly.

Changing Display Size for Windows-based Client Sessions

You can set a user preference to specify the default window size for remote sessions to adjust to different display requirements. For example, if you are viewing sessions using a tablet or a computer with a small monitor you might want to change the display size to suit a smaller screen than when you are working with a full-scale desktop monitor.

If you have administrative rights for the Privileged Access Service, you can change the window size for remote sessions from the Admin Portal by setting a user preference.

For more information about changing the window size for Windows-based client sessions, see "Selecting User Preferences" on page 764

Downloading and Testing the Remote Access Kit

If you want to use the local Windows-based client for remote sessions, you can download and install the **Remote Access Kit** for Windows computers. After you have downloaded and installed the software package or if you need to verify access to it on a specific local computer, you can test for the availability of the program before you attempt to open sessions using the local Windows-based client.

if you have administrative rights for the Privileged Access Service, you can download, install, and test access to the remote access kit from the Admin Portal by setting a user preference.

For more information about changing the window size for Windows-based client sessions, see "Selecting User Preferences" on page 764

To download and install the Remote Access Kit:

1. In the Admin Portal, click **Settings**, then click **Resources** to display the settings available for the Infrastructure Services.
2. Click **User Preferences**.
3. Select the local Windows-based client to use for SSH and RDP sessions.
4. Click **Download** to download the Remote Access Kit software package that contains the local client launcher.
5. Open the downloaded file and follow the prompts displayed to install the software.
6. Click **Save**.
7. Downloading the installing the Remote Access Kit automatically downloads the RDP file for launching a Windows Remote Desktop Connection.
8. If you want to immediately verify installation on the local computer, select **I have installed the Remote Access Kit on this computer** then click **Test**.
9. Click **Open Delinea Remote Access Kit** to complete verification.
10. If you trust the website URL for the current cloud server, click **Yes**.

If you do not download and install the Remote Access Kit on the local computer, review the instructions displayed for information about how to start sessions using the local Windows-based client with command-line arguments.

To test for the availability of the Remote Access Kit:

1. In the Admin Portal, click **Settings**, then click **Resources** to display the settings available for the Infrastructure Services.
2. Click **User Preferences**.
3. Select **I have installed the Remote Access Kit on this computer**.
4. Click **Test**.
5. If you have installed the Remote Access Kit on the local computer, you are prompted to open it.
6. Click **Open Delinea Remote Access Kit** to complete verification.
7. If you trust the website URL for the current cloud server, click **Yes**.

If you do not download and install the Remote Access Kit on the local computer, review the instructions displayed for information about how to start sessions using the local Windows-based client with command-line arguments.

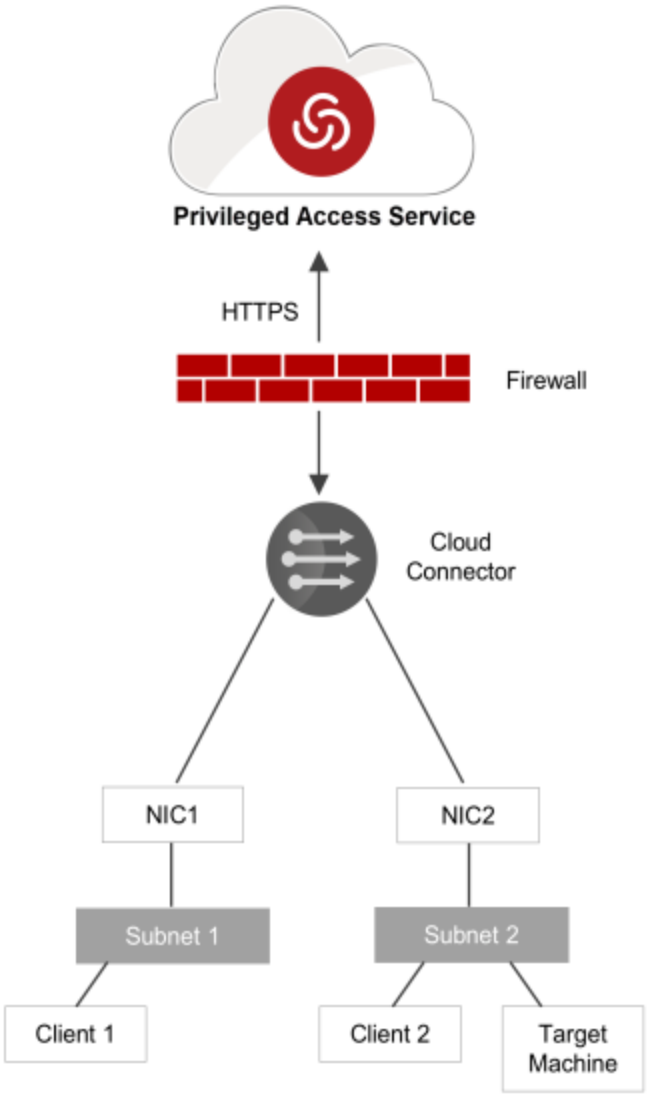
Using Multiple NICs

In an environment where the connector has multiple network interface cards (NICs) with multiple subnets, there are differences in the way RDP or SSH clients and target computers interact with the connector to determine the appropriate IP address to use for the remote session.

Local Windows-based clients using the Remote Access Kit Local Client Launcher – If you are using a local Windows-based client with the Remote Access Kit, the local client launcher application sends all the IP addresses from the NICs simultaneously to the client. The client then uses the first successful IP address it receives from the local client launcher to open its SSH or RDP connection. The Remote Access Kit local client launcher helps to resolve all of the IP addresses available to determine the most appropriate IP address to use for the connection. As illustrated in the diagram below, if you have a connector with multiple network interfaces and Client 1 is a local Windows-based client that uses the Remote Access Kit local client launcher, the local client launcher resolves the IP addresses from NIC 1 and NIC 2 simultaneously. If Client 1 needs to open a remote connection to a target, it has access to both network interfaces and uses the first successful IP address connection returned to start the SSH/RDP session. For information about how to download and install the Remote Access Kit software package that includes the local client launcher, see "Selecting User Preferences" on page 764

Local Windows-based clients without the Remote Access Kit – The Remote Access Kit local client launcher is an optional application. If you are not using the Windows-based client with the Remote Access Kit local client launcher, the client tries to connect to each IP address one at a time. This single-track process can delay a successful IP address connection. The client must also be able to resolve the connector's fully-qualified domain name (FQDN) using your DNS server. If the DNS server returns multiple connector IP addresses to the RDP or SSH client, the local client–such as PuTTY or MSTSC–determines whether the connection is a single-track or multiple track process. In this environment, the local client resolves the connection to the fully-qualified domain name (FQDN) of the connector that it should use. As illustrated in the diagram below, if Client 1 does not use the Remote Access Kit local client launcher and needs to open a remote connection to a target, it tries to connect using the IP address from NIC 1 first. If the attempt to connect to the NIC 1 IP address is not successful, then the client tries to connect using the IP address from NIC 2.

Direct connections from target systems – You can configure Delinea PAS to connect directly to target systems from the connector for RDP or SSH sessions. Configuring a direct connection requires that you have at least one NIC that can communicate with the target system. For information about how to configure a direct connection from the target system to the connector, see "Selecting Connectors" on page 555 Alternatively, you can map system subnets to specific connectors. For information about how to configure specific subnets for a connector, see "Mapping System Subnets to Connectors" on page 760



Note: To use native SSH/RDP with a single NIC or multiple NICs, the connector must have at least one NIC that can connect to the client or target system.

Configuring Policy Settings

You can use the policy system in **Admin Portal > Access > Policies** to create policy rules for users and resources added to Privileged Access Service. The Policy System allows you to configure options in the following areas:

- "Authentication Policies" on page 723

  You can configure authentication policy controls for web logins to Centrify PAS and build rules to define authentication challenge requirements, You can also configure authentication policy controls for Windows and Linux clients, Privilege Elevation Service for UNIX (dzdo), and Privilege Elevation.

- "User Security Policies" on page 727

  You can configure policy controls for Self Service Controls, user password management, OATH OTP integration, User Account Settings, and RADIUS client security policies.

- "Resource Policies" on page 736

  You can configure policy controls and apply to sets of resources added to Centrify PAS.

- "Third Party Integration Policies" on page 736

  You can configure policy rules to define authentication challenge requirements for third party integrations.

- "Device Policies" on page 737

  You can configure policy controls for device registration and usage.

Policy Assignments

Policy can be applied to users and resources by the following assignment options:

- **Everything** policy assignment that applies to everything.
- **Specified Roles** policy assignment that applies to roles you specify.
- **Sets** policy assignment that applies to specific sets.

For more information on policy assignments, see "Creating Policy Sets and Policy Assignments" on the next page.

Depending on the policy assignment you choose, certain policy settings may not be available. For example, if you choose the Sets policy assignment and choose Systems as the set type, you will only see policy settings that apply to system resources.

Note: Policy assignment settings cannot be changed once the policy set is saved.

Policy Hierarchy and Overrides

Policy sets are applied to users and resources from top to bottom when viewing the Policy Sets on the Policy page. If the same policy has different settings in different policy sets, the setting in the first policy set – the top-most – is applied.

You can apply multiple policy sets to the same role or the same resource set. For example, you might create a policy to define basic policies for Everything (all users and resources) and then create more policy sets for a subset of those users or resources. If you want one policy setting to be enforced over another one, drag that policy set up in the list.

If more than one system administrator is updating the same policy or re-prioritizing the policy sets, the changes made first (by clicking the Save button or dragging the policy set) will be saved. The administrator who's changes were not saved must refresh the policy and make the changes again.

Configuring policy settings for resources are available in various locations in the Admin Portal: **Settings > Resources > Security Settings** , **Access > Policies > Resources**, and **Resources > Policies**.

In most cases, you can override global settings (configured in the Access or Settings page) for individual resource in the specific Policy page for the resource (**Resources > Policies**). The global settings only apply where you have not explicitly configured a setting for an individual resource. Centrify PAS prioritizes the policy settings using the following order:

1. Account overrides configured in **Resources > Accounts > Policies**
2. Account policy settings configured in **Access > Policies > Resources > Accounts**
3. Resource overrides configured in the **Resources > Systems > Policies**
4. Resource policy setting configured in **Access > Policies > Resources > Systems**
5. Resource Global policies configured in **Settings > Resources > Security Settings**
6. System default value.

> **Note:** If the account is a domain or database account, all references to “system” are “domain.”

Policy Summary

Policy summary pages are available to view policy allocation for users and resources. You can access policy summary pages in the following locations in the Admin Portal:

- Policy Set: **Access > Policies > [select policy set] > Summary**

  Displays the current policy configuration settings for the set but does not show the default value for policies you have not modified.
- Resource overrides: **Resources > [select resource] > Policy Summary**

  Displays the policy settings and overrides for an individual resource. These policies are set at the resource. By default, the summary is for the logged-in user viewing the summary as shown in the selected user field at the top of the screen.
- Specific user: **Access > Users > [select user] > Policy Summary**

  Displays the policy settings for an individual user.

Creating Policy Sets and Policy Assignments

The following procedure provides information on how to create a policy set and apply a policy assignment.

To create a policy set and specify the policy assignment:

1. Log in to Admin Portal.
2. Click **Access > Policies > Add Policy Set**.
3. Enter a name for the policy set.

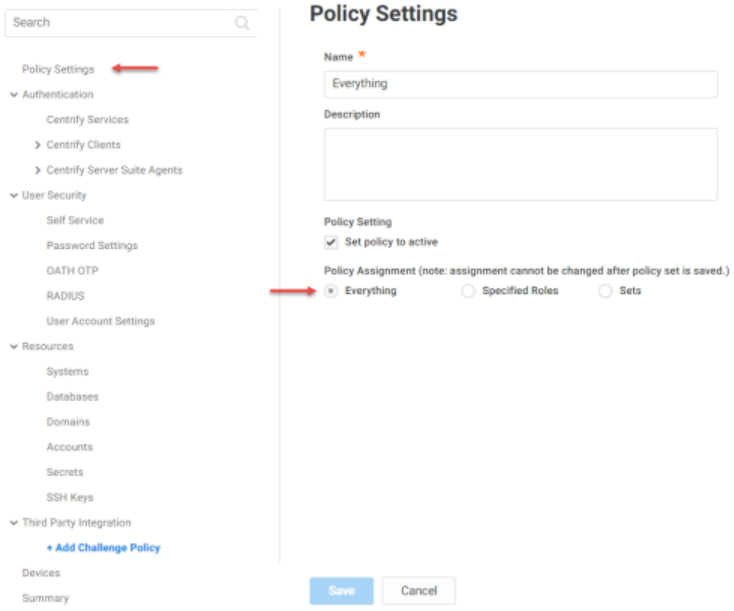
> **Note:** You can use uppercase and lowercase characters, spaces, numbers, and most special characters (you cannot, for example, use the forward and backward slash). The Name text box outline turns red if you enter an illegal character.

4. Enter the **Description** you want to appear on the Admin Portal Policy page.
5. Configure the **Set policy to active** option if necessary. This option is enabled by default.
6. Specify the policy assignment:

> **Note:** Policy settings available change based on what option you select here (i.e., Everything, Specified Roles, Sets). This is because only some policies are user specific, while almost all of them are non-user specific.

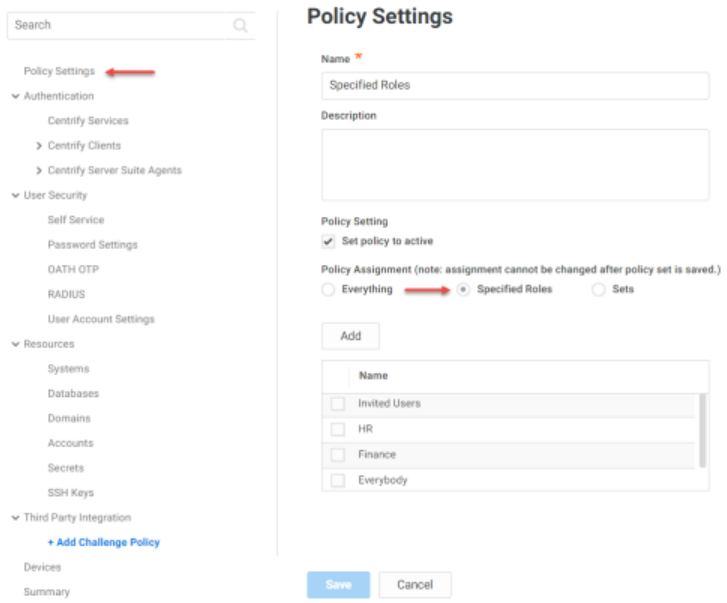
- Everything

  Applies this policy to all users registered in Privileged Access Service and all resources added to the Privileged Access Service. The following is an example of the policies available:



- Specified Roles

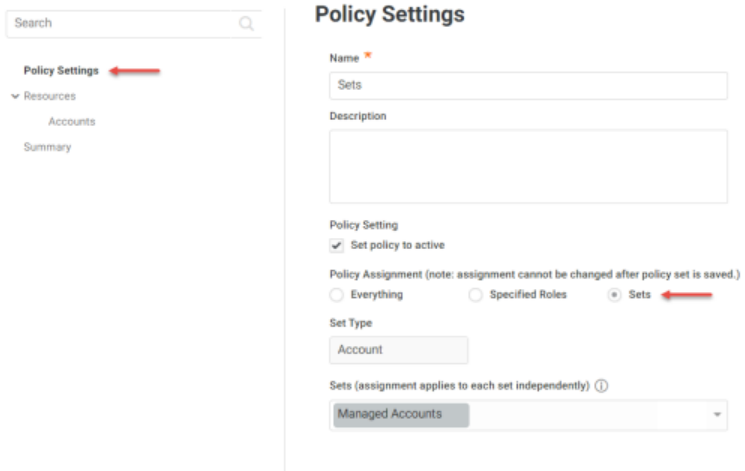
  Click **Add** to select the Roles (see Adding roles to configure roles in the Admin Portal) to which you want this policy applied. All current and subsequent policy settings apply to the roles selected. The following is an example of the policies available:



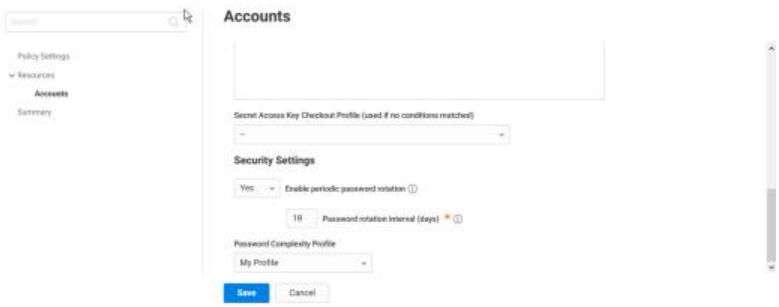
- Sets

  Specify the set type (this applies to the following resource types: Account, Database, Domains, Secrets, SSH Keys, Systems) and then select or enter the sets to which you want to apply policy settings. This assumes you have already configured sets for the specified Set type. For information on creating sets for resources, see Managing sets.

  Note: Only the policy settings that apply to the particular set are available for configuration. See the following example:



To configure the password rotation time and complexity:



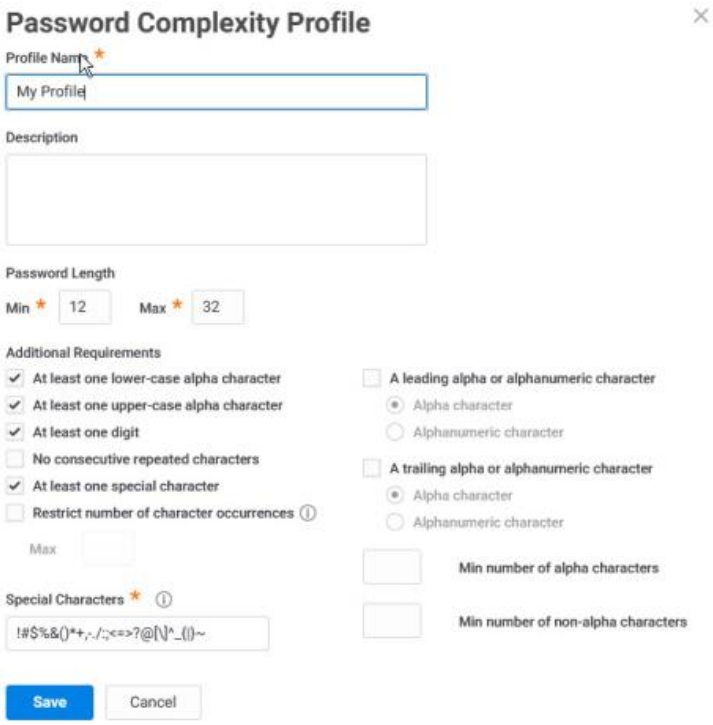
a. Click **Accounts** from the left menu.

b. Scroll to Security Settings and set Enable periodic password rotation to **Yes** and enter the desired value for **Password rotation interval (days)**.

c. Select **Add New Profile** from the Password Complexity Profile dropdown menu.

d. Read the Confirm password profile alert and click **Continue**.

e. Complete the Password Complexity Profile information and click **Save**.



7. Click **Save**.

Using Hierarchical Policy Sets

You can apply multiple policy sets to the same role. For example, you might create a global policy set to define basic policies for all users and then create more policy sets for a subset of those users.

Privileged Access Service reads the policy sets from bottom to top on the Policy page when it installs the policies in a device. If the same policy has different settings in different policy sets, the setting in the last policy set – the top-most – is applied.

For users in multiple roles or collection parameters, the Privileged Access Service first determines which policy sets apply to the user and then reads those policy sets from bottom to top to apply the policies. The hierarchical order of the roles has no effect upon the order in which the policy sets are read.

If you want one policy setting to be enforced over another one, drag that policy set up in the list.

If more than one system administrator is updating the same policy or re-prioritizing the policy sets, the changes made first (by clicking the Save button or dragging the policy set) will be saved. The administrator who's changes were not saved must refresh the policy and make the changes again.

Authentication Policies

In the **Admin Portal Access > Policies > Authentication** tab, you can configure the following policies:

- "Authentication Policy for Centrify Services" below – applies to all web logins to the Privileged Access Service, including the Admin Portal and on-demand application authentication.
- "Cloud Clients Policies" on page 725 – enable authentication policy controls for Cloud Clients.
- "Centrify Server Suite Agents Policies" on page 726 - applies to:
  - Linux, UNIX, and Windows servers - applies to Centrify-managed Windows, UNIX and Linux Servers. Also applies to UNIX and Linux Workstations.
  - Windows workstations - applies to Centrify-managed Windows Workstations.
  - Privilege Elevation - applies to Privilege Elevation Service for UNIX (`dzdo') and Privilege Elevation Service for Windows ('Run with Privilege').

Authentication Policy for Centrify Services

You can enable users to perform certain tasks related to their accounts.

To access and enable the Centrify Services options:

1. Log in to Admin Portal, click **Access > Policies**, and select the policy set.
2. Click **Authentication > Centrify Services**.
3. Select **Yes** in the "Enable authentication policy controls" drop-down.

Once enabled, you can configure the following options:

Authentication Rules

Available Settings	Description
Authentication Rules	Build rules to define conditions for authentication challenge requirements. Each rule maps to a customizable authentication profile. The default profile is used if no rules are configured.
Default Profile	The profile Centrify PAS uses if no profile is added/selected.

Session Parameters

Available Settings	Description
Hours until session expires (default 12)	The number of hours that Privileged Access Service accepts a previous log in from the same browser for authentication
Allow 'Keep me signed in' checkbox option at login (session spans browser sessions)	Enables the option to select 'Keep me signed in' at login.
Default 'Keep me signed in' checkbox option to enabled	Option that allows “Keep me signed in” checkbox enabled by default for users.
Hours until session expires when 'Keep me signed in' option enabled (default 2 weeks)	Number of hours "Keep me signed in” checkbox enabled by default for users. Default is 2 weeks.

Additional Centrify Services Parameters

Available Settings	Description
Allow IWA connections (bypasses authentication rules and default profile)	Allows Centrify PAS to bypass already configured authentication rules and default authentication profiles when IWA is configured. This option is configured by default.
Set identity cookie for IWA connections	Enables Centrify PAS to write a cookie in the current browser after a successful IWA-based log in. Centrify PAS checks the browser for this cookie when the user logs in to the Admin Portal. As long as the cookie is there, the user is not prompted for multi-factor authentication.
IWA connections satisfy all MFA mechanisms	This option tells the Privileged Access Service to allow IWA to override all application specific authentication requirements.
Use certificates for authentication	Allows you to use certificate for authentication.
Certificate authentication bypasses authentication rules and default profile	When this setting is disabled, an Authentication Rule that contains a "Certificate Authentication" filter will challenge users with the selected Authentication Profile after certificate authentication succeeds.

Available Settings	Description
Set identity cookie for connections using certificate authentication	Allows you to log in using smart cards and another authentication method.
Connections using certificate authentication satisfy all MFA mechanisms	Connections using certificate authentication satisfy all MFA mechanisms.
Allow users without a valid authentication factor to log in	Exempts users from multifactor authentication when their account does not have a mobile phone number and email address.
Apply additional authentication rules to federated users	When enabled, additional authentication rules are applied to federated users. Federated IDP authentication satisfies the password mechanism in these cases.
Connections via Federation satisfy all MFA mechanisms	When enabled, if a user is successfully authenticated via Federation then they will not be challenged with additional MFA mechanisms.
Allow additional authentication from same device	Disabling this option blocks all authentication methods to the same device except Password, Email, Security Questions, and 3rd Party RADIUS.
Continue with additional challenges after failed challenge	Notifies users of a failed authentication after the first failed challenge.
Do not send challenge request when previous challenge response failed	Configure Centrify PAS to handle the default MFA behavior (allow users to step through all the relevant MFA challenges before we notify them of their failed authentication attempt) differently based on the challenge type.
Remember and suggest last used authentication factor	To remember the last used authentication method.

Cloud Clients Policies

You can enable users to perform certain tasks related to their accounts.

To access and enable the Cloud Clients options:

1. Log in to Admin Portal, click **Access > Policies**, and select the policy set.
2. Click **Authentication > Centrify Clients > Login**.
3. Select **Yes** in the "Enable authentication policy controls" drop-down.

Once enabled, you can configure the following options:

Authentication Rules

Available Settings	Description
Add Rule	Build rules to define conditions for authentication challenge requirements. Each rule maps to a customizable authentication profile. The default profile is used if no rules are configured.
Default Profile	The profile Centrify PAS uses if no profile is added/selected.

Additional Centrify Client Parameters

Available Settings	Description
Allow users without a valid authentication factor to log in	To exempt users from multifactor authentication when their account does not have a mobile phone number and email address.

Centrify Server Suite Agents Policies

You can enable users to perform certain tasks related to their accounts.

To access and enable the Centrify Server Suite Agents options:

1. Log in to Admin Portal, click **Access > Policies** and select the policy set.
2. Click **Authentication > Centrify Server Suite Agents**. From here, you can choose from one of the following:
   - Linux, UNIX and Windows Servers.
   - Windows Workstations.
   - Privilege Elevation.
3. Select **Yes** in the "Enable authentication policy controls" drop-down.

Once enabled, you can configure **Authentication Rules and Default Profile** and **Apply Pass-Through Duration**.

Authentication Rules and Default Profile

Available Settings	Description
Add Rule	Build rules to define conditions for authentication challenge requirements. Each rule maps to a customizable authentication profile. The default profile is used if no rules are configured.
Default Profile	The profile Centrify PAS uses if no profile is added/selected.

Apply Pass-Through Duration

For Linux, UNIX and Windows Servers, there are additional pass-through duration settings. Pass-through refers to situations where a user logs in to multiple systems, and whether or not their authentication is "passed-through" to the secondary system. The authentication profile that you specify here controls the authentication timeout.

- **Never (Default)** - Prompt for MFA every time, irrespective of the chosen profile's Pass-through setting.
- **If Same Source and Target** - Allow pass-through as long as source and target system remain unchanged.
- **If Same Source** - Allow pass-through as long as source system remains unchanged.
- **If Same Target** - Allow pass-through as long as target system remains unchanged.

User Security Policies

In the **Admin Portal Access > Policies > User Security** tab, you can configure the following policies:

- "Self Service" below - In Self Service you configure parameters for password reset and account unlock.
- "Password Settings" on page 730 - In Password Settings you configure parameters for password rule requirements and manage password age and capture settings.
- "OATH OTP" on page 732 - In OATH OTP you enable OATH OTP integration.
- "RADIUS" on page 733 - In RADIUS you enable RADIUS client connections and set security policies.
- "User Security User Account Settings" on page 733 - In User Account Settings you enable additional account parameters, such as allowing users to change their passwords, enroll FIDO2 authenticators, configure security questions etc.

Self Service

You can enable users to perform certain tasks related to their accounts. If you want to enable these features for Active Directory users, you need to run the Centrify Connector under an account with the necessary permissions and follow these procedures.

To access and enable the Self Service options:

1. Log in to Admin Portal, click Access > Policies, and select the policy set.
2. Click User Security > Self Service.

3. Select Yes in the "Enable account self service controls" drop-down.

Once enabled you can configure the following options:

Password Reset

Available Settings	Description
Enable password reset	Click the check box to allow users to reset their passwords and specify additional authentication requirements for password reset.
Allow for Active Directory users	Enables users with Active Directory accounts who have forgotten their password to log in and reset their password. If you do not set this option, the “Forgot your password?” link is not displayed in the login prompt for users with Active Directory accounts. If you set this option, then you need to configure the Active Directory Self Service Settings on this page.
Only allow from browsers with identity cookie	Restricts password reset to those users who have already logged in successfully. If this check box is not enabled, then anybody can use the password reset options. The Privileged Access Service writes the identity cookie the first time the user logs in successfully. However, when users clear the history on their browsers, it removes this cookie.
User must log in after successful password reset	Requires the user to log in after a password reset.
Password Reset Authentication Profile	Configure password reset self-service options
Maximum consecutive password reset attempts per session	This option specifies the number of attempts users have to reset their password for that session before they are taken back to the log-in page. The default is 5 attempts.

Account Unlock

Available Settings	Description
Enable account unlock	You can enable users to unlock their accounts.
Allow for Active Directory users	Enables users with Active Directory accounts to unlock their accounts. If you do not set this option, the “Unlock your account?” link is not displayed in the login prompt for users with Active Directory accounts. If you set this option, then you will need to configure the Active Directory Self Service Settings.

Available Settings	Description
Only allow from browsers with identity cookie	Restricts account unlock to those users who have already logged in successfully. If this box is not set, anybody can use the account unlock option. The Privileged Access Service writes the identity cookie the first time the user logs in successfully. However, when users clear the history on their browsers, it removes this cookie.
Show a message to end users in desktop login that account is locked (default no)	Option to display a message that the account is locked.
Account Unlock Authentication Profile	Configure account unlock self-service options

Active Directory Self Service Settings

Available Settings	Description
Use connector running on privileged account	To run the connector under an account that has the User Account Control permission. Unless you have changed the connector account after you ran the connector installation wizard, the connector is run as a Local System account process. By default, a Local System account does not have the User Account Control permission. See Permissions required for alternate accounts and organizational units to set the permission. Optionally, after you select this Use connector running on privileged account setting, you can assign account unlock permission for Active Directory users by creating a security group in Active Directory, give a user or group permission to read and write the LockoutTime attribute for an OU or other container, and add the connector's computer object(s) to that group.
Use these credentials	Select this option and provide the account user name and password to use an account with the required permission to unlock the account. For example, any account in the connector's Domain Admins group can unlock another user's Active Directory account.

Additional Policy Parameters

Available Settings	Description
Maximum forgotten password resets allowed within window (default 10)	Set a maximum for the number of times users can reset their password within the capture window. If users exceed this limit, the next time they attempt to reset the password, they get a message that they have reset their password too often and must wait before attempting again.

Available Settings	Description
Capture window for forgotten password resets (default 60 minutes)	Set the time period for maximum forgotten password resets. When users exceed the number or resets in this time period, they cannot reset the password again. This value also specifies how long from the last reset attempt the user must wait before they are allowed to reset the password.

Password Settings

You can enable users to perform certain tasks related to their accounts.

To access and enable the Password Settings options:

1. Log in to Admin Portal, click **Access > Policies**, and select the policy set.
2. Click **User Security > Password Settings**. Once enabled you can configure the following options:

Password Requirements

Available Settings	Description
Minimum password length (default 8)	Use the drop-down list to select the minimum length required for a password or "--" to use the default setting, which is 8.
Maximum password length (default 64)	Use the drop-down list to select the maximum length required for a password or "--" to use the default setting, which is 64.
Require at least one digit (default yes)	Select Yes to require the user to have at least one digit in the password, No to require no digits in the password, or "--" to use the default setting, which is Yes.
Require at least one upper case and one lower case letter (default yes)	Select Yes to require the user to have at least one upper case and one lower case (total two letters) in the password, No to require no letters in the password, or "--" to use the default setting, which is Yes.
Require at least one symbol (default no)	Select Yes to require at least one symbol, No to require no symbols, or "--" to use the default setting. The default is No.

Display Requirements

Available Settings	Description
Show password complexity requirements when entering a new password (default no)	Enabling this policy displays the password complexity requirements when updating a user account password. The default value "--" is equivalent to No.
Password complexity requirements for directory services other than Centrify Directory	Password complexity requirements for Centrify Directory users are automatically discovered but all other directory services require manually entering a complexity requirement string.

Additional Password Setting Requirements

Available Settings	Description
Limit the number of consecutive repeated characters	Password cannot contain consecutive repeated characters equal to or more than the set value. The default is to allow consecutive repeated characters.
Check against weak password	Select Yes to check password-strength, No to save password without password-strength checking, or "--" to use the default setting, which is No.
Allow username as part of password	Select Yes to allow username in the password, No to disallow username in the password, or "--" to use the default setting, which is Yes.
Allow display name as part of password	Select Yes to allow part of displayname in the password, No to disallow part of displayname in the password, or "--" to use the default setting, which is Yes.
Require at least one Unicode characters	Select Yes to require the user to have at least one unicode in the password, No to require no unicode in the password, or "--" to use the default setting, which is No.

Password Age

Available Settings	Description
Minimum password age before change is allowed (default 0 days)	The default is 0 days. Users will not be allowed to change or reset their password until the current password is at least this old.
Maximum password age (default 365 days)	The default is 365 days. After the password expires, users are prompted to enter their current password and then enter a new one. Enter 0 (zero) if you do not want to specify a password expiration period.
Password history (default 3)	Use the drop-down list to select the number of most recent passwords to save or "--" to use the default setting. The user cannot re-use the passwords on this list. The number you enter is displayed in the message when the user is prompted to enter a new password.
Password Expiration Notification (default 14 days)	Select the number of days before a user's password expires to begin posting a notification of expiration through a portal banner and daily emails. This policy applies to Centrify Directory users and Active Directory accounts.

Available Settings	Description
Escalated Password Expiration Notification (default 48 hours	Select the number of hours before a user's password expires to present a change password dialog. The dialog is automatically displayed when the user logs in. This policy applies to Centrify Directory users and Active Directory accounts. **Note**: This policy is not supported on mobile clients.
Enable password expiration notifications on enrolled mobile devices	When enabled, password expiration notifications are sent to registered mobile devices. The default setting "--" is equivalent to Yes.

Capture Settings

Available Settings	Description
Maximum consecutive bad password attempts allowed within window (default Off)	Use the drop-down list to select the number of failed password attempts allowed within the period you specify in the "Capture window for consecutive bad password attempts" policy before the user is locked out, Off to allow the user an unlimited number of failed attempts, or "--" to use the default setting. Users are locked out for the time period you specify in the "Lockout duration before password re-attempt allowed" policy when they fail in the attempt after the number you select.
Capture window for consecutive bad password attempts (default 30 minutes)	Enter the number of minutes to define the time period before the number of failed password attempts is reset. This time period is only applicable when the "Maximum consecutive bad password attempts allowed within window" policy defines the number of failed attempts allowed and is not set to Off. The user is locked out for the time period you set in the "Lockout duration before password re-attempt allowed" policy. After that, the user can attempt to log in again.
Lockout duration before password re-attempt allowed (default 30 minutes)	Enter the number of minutes users must wait before they can attempt to log in again after lockout.

OATH OTP

You can enable users to perform certain tasks related to their accounts.

To access and enable the OATH OTP options:

1. Log in to Admin Portal, click **Access > Policies**, and select the policy set.
2. Click **User Security > OATH OTP**.
3. Select **Yes** in the "Allow OATH OTP integration" drop-down and click **Save**.

RADIUS

You can enable users to perform certain tasks related to their accounts.

To access and enable the Radius options:

1. Log in to Admin Portal, click **Access > Policies**, and select the policy set.
2. Click **User Security > Radius** where you see the following options:

Radius Policies

Available Settings	Description
Allow RADIUS client connections	This enables you to extend MFA from Privileged Access Service to thick clients (such as VPNs) that support RADIUS.
Require authentication challenge	Requires you to set a challenge.
Add Auth Profile	Add an authorization profile.
Default Authentication Profile	The default authentication profile.
Send vendor specific attributes	Allows you to select and send vendor-specific attributes.
Add Attributes	Select the attributes you want to send.
Allow 3rd Party RADIUS Authentication	This enables you to add 3rd party authentication solutions (example: RSA SecurID) to the list of supported authentication mechanisms for your users.

User Security User Account Settings

You can enable users to perform certain tasks related to their accounts.

To access and enable the User Account Settings options:

1. Log in to Admin Portal, click **Access > Policies**, and select the policy set.
2. Click **User Security > User Account Settings** where you see the following options:

User Account Settings

Available Settings	Description
Enable users to redirect multi factor authentication to a different user account	This policy determines whether a user can choose to have multi factor authentication redirected to a different user account. This is useful for users who have more than one user account but prefer to use one mobile phone for authentication. The default value "--" is equivalent to No.
Authentication Profile required to modify personal profile	The authentication profile that a user needs in order to modify their personal profile.
Default language	This language will be used for displaying the portal and all communications if a user has not set their own preferred language. If this policy is not set, the user's browser culture will be used if available.

User Security Authentication Settings

You can enable users to perform certain tasks related to their accounts.

To access and enable the User Security Authentication Settings options:

1. Log in to the Admin Portal, click **Access > Policies**, and select the policy set that you want to edit.
2. Click **User Security > Authentication Settings** where you see the following options:

Authentication Settings

Available Settings	Description
Enable users to change their passwords	This policy determines whether users can change their passwords from the Account page, and is independent of the policies available under Password Reset. The default value "--" is equivalent to Yes.
Authentication Profile required to change password	The profile needed to change password.
Enable users to enroll FIDO2 Authenticators	This policy determines whether users can enroll FIDO2 authenticators to authenticate to Cloud Suite. Select Yes to display the Security Key and On-device Authenticator options to users. Select no to hide the Security Key and On-device Authenticator options from users. The default value “—” is equivalent to No.
Require users to configure FIDO2 Security Key at sign in	If set to yes, users must configure a FIDO2 security key after they log in and before they can access other areas of the Admin Portal.
FIDO2 Security Key Display Name	Enter a name that will be familiar to your users (such as the name of the FIDO2 Security Keys used by your organization).

Available Settings	Description
Authentication Profile required to configure FIDO2 Authenticators	The profile needed to configure FIDO2 Authenticators.
Enable users to configure an OATH OTP client (requires enabling OATH OTP policy)	This policy is typically used when you bulk upload OATH tokens (for example, those generated by a YubiKey). Select Yes to display the QR code to users. Select No to hide the QR code from users. The default value "--" is equivalent to Yes. **Important**: If you choose to not display the QR code, users without an enrolled device will not be able to scan the QR code and get a passcode pushed to their devices. In order for this policy to take effect, you also have to set the Security > OATH OTP > Allow OATH OTP policy to Yes.
Require users to configure at sign in	If set to yes, users must configure an OATH OTP client after they log in and before they can access other areas of the Admin Portal.
OATH OTP Display Name	Enter a name that will be familiar to your users (such as the name of the OTP Client used by your organization). This value will be used throughout the UI wherever users configure or use an OTP Client. NOTE: this is only a label and does not prevent users from using other OATH Clients.
Authentication Profile required to configure OATH OTP client	The profile needed to configure OATH OTP client
Enable users to configure Security Questions	This policy determines whether configuring security questions is required for users to authenticate using security question. The default value is enabled and requires that users configure one security question.
Require users to configure at sign in	If set to yes, users must configure their security questions before they can access any areas of theAdmin Portal after they log in.
Allow duplicate security question answers	Existing questions will remain, allowing duplicate answers if already provided before the policy/config is disabled.
Required number of user-defined questions	Specifies the number of questions from the user generated security questions list that must be configured by users.

Available Settings	Description
Required number of admin-defined questions	Specifies the number of questions from the admin generated security questions list that must be configured by users.
Minimum number of characters required in answers	The minimum number of characters required in answers.
Authentication Profile required to set security questions	The authentication profile required to set security questions.
Require users to register device at sign in to use Mobile Authenticator (requires Permit Device Registration policy in Devices)	If set to yes, users must register their mobile device when they log in so that they can use the Mobile Authenticator app. In order for this policy to take effect, you also have to set the Devices > Permit Device registration policy to Yes.

Resource Policies

In the **Admin Portal Access > Policies > Resources** tab, you can configure parameters for the following resources:

- "Setting System-Specific Policies" on page 641
- "Setting Database-Specific Policies" on page 670
- "Setting Database-specific Policies" on page 485
- "Accessing Accounts" on page 456
- "Setting Access Challenge Policies" on page 640
- "Adding SSH keys" on page 512
- "Managing a Cloud Provider Account" on page 567

When you configure policy settings in **Access > Policies > Resources**, you are configuring policies for all resources or a set of resources. To configure policy settings for individual resources or override these settings, you need to access the individual resource and access the Policy or Advanced tab for that resource. For instance, to override a System policy configuration set in **Access > Policies > Resources**, you would access **Resources > Systems** and then select the individual system Policy or Advanced tab.

Third Party Integration Policies

In the **Admin Portal Access > Policies > Third Party Integration** tab, you can add and manage challenge policy controls. You can also enable users without a valid authentication factor to log in.

To access and enable the Third Party Integration options:

1. Log in to Admin Portal, click **Access > Policies**, and select the policy set.
2. Click **Third Party Integration > Add Challenge Policy**. Click **Add Challenge Policy**.

3. Select **Yes** in the "Enable authentication policy controls" drop-down.

   Once enabled, you can configure the following options:

Authentication Rules

Available Settings	Description
Authentication Rules	Build rules to define conditions for authentication challenge requirements. Each rule maps to a customizable authentication profile. The default profile is used if no rules are configured.
Default Profile	The profile Centrify PAS uses if no profile is added/selected.

Additional Third Party Integration Options

Available Settings	Description
Allow users without a valid authentication factor to log in	To exempt users from multifactor authentication when their account does not have a mobile phone number and email address

Device Policies

In the **Admin Portal Access > Policies > Devices** tab, you can register devices and configure parameters for those devices. When devices are registered, you can manage them from the Admin Portal.

To access and enable the Device options:

1. Log in to Admin Portal, click **Access > Policies**, and select the policy set.
2. Click **Devices** and you will see the following options:

Devices

Available Settings	Description
Permit device registration	Select Yes to allow users to register devices, No to prevent users from registering devices, or “--” to use the default setting. The default is Yes.
Permit non-compliant devices to register	Select Yes to allow users to register non-compliant devices, No to prevent the user from registering non-compliant devices, or "--" (Not configured) to use the default setting. This policy must be set to Yes to bypass the Google services SafetyNet check and allow registration of the device. Notes: This policy is enforced by the registration application running on the device. If the user uses web registration instead of an application, this policy is not enforced. This policy is not supported on OS X and Android devices earlier than version 2.3.

Available Settings	Description
Enable invite based registration	Click Yes to enable users to register devices using invite based registration, No to disable the policy, or "--" (equivalent to No) to use the default setting. You must select Yes to allow users to register their devices using the system generated QR code.
Allow user notifications on multiple devices	Select Yes to send authentication notifications to multiple registered devices, No to send to the first registered device only (default setting), or "--" to use the default setting.
Enable debug logging	There are two logging modes on devices: regular - the default setting - and debug logging. Use this policy to turn on the debug logging mode. Select Yes to enable debug logging, No to set regular logging, or "--" (Not configured) to use the default setting.
Report mobile device location	Select Yes to allow devices to report their location, No to stop the device from reporting location, or "--" to use the default setting (Yes).
Enforce fingerprint scan for Mobile Authenticator	Select Yes to require that users provide a finger print scan to use mobile authenticator. Using the associated policy option, users can alternatively use the client application PIN for access. The default setting is No.
Allow App PIN	Select Yes to allow users to access the mobile authenticator code using finger print or the client application PIN. The default setting is No.
Require client application passcode on device	Select Yes to require a passcode to open the client application, No to allow opening the client application without a passcode, or "--" (Not configured) to use the default setting. Important: You must select Yes to enable other client application passcode policies.
Auto-Lock (minutes)	Select a value from the "Auto-Lock (minutes)" drop-down list to set the number of minutes of inactivity before the client application is locked. Select "--" (Not configured) to use the default setting. Important: The "Require client application passcode on device" policy must be set to Yes to enforce this policy.
Lock on exit	Select Yes to require a passcode to open the client application after the client has been closed, No to allow opening the client application without a passcode, or "--" (Not configured) to use the default setting. Important: The "Require client application passcode on device" policy must be set to Yes to enforce this policy.

How to Select the Policy Service for Device Management

You can use Centrify directory policy service or Active Directory Group Policy Management to set device configuration policies. When you select the Centrify directory policy service, you use policy sets created in Admin Portal to set device configuration policies. When you use Active Directory group policy, you create group policy objects and edit them with the Group Policy Management Editor to set device configuration policies. You use roles

to apply the policies to sets of users by linking the group policy object to an Active Directory organizational unit and then specify that organizational unit in the device registration settings.

Note: You must use Privileged Access Service for mobile device management if you want to set the mobile device policies and install them in the device.

Both methods provide largely the same policies. The method you select depends upon the types of accounts (Centrify Directory or Active Directory) used for registering devices. Use the following guidelines to select the proper method for your organization:

You have devices registered by users with the following types of accounts	Select this method	Notes
Both users with Centrify Directory and Active Directory accounts	Centrify directory policy service	If you select Active Directory, Privileged Access Service does not install the policies in devices registered by users with Centrify Directory accounts.
Only users with Active Directory accounts	Either Active Directory or Centrify directory policy service	Select the method that is most convenient to you.
Only users with Centrify Directory accounts	Centrify directory policy service	

Note: If you select Active Directory group policy, you still use policy sets to configure the Device Management Settings, Device Registration Settings, User Security Policies, and Application Policies. You use the group policy object just to set the device configuration policies (Policies > Endpoint Policies > settings in Common Mobile Settings, iOS Settings, etc.).

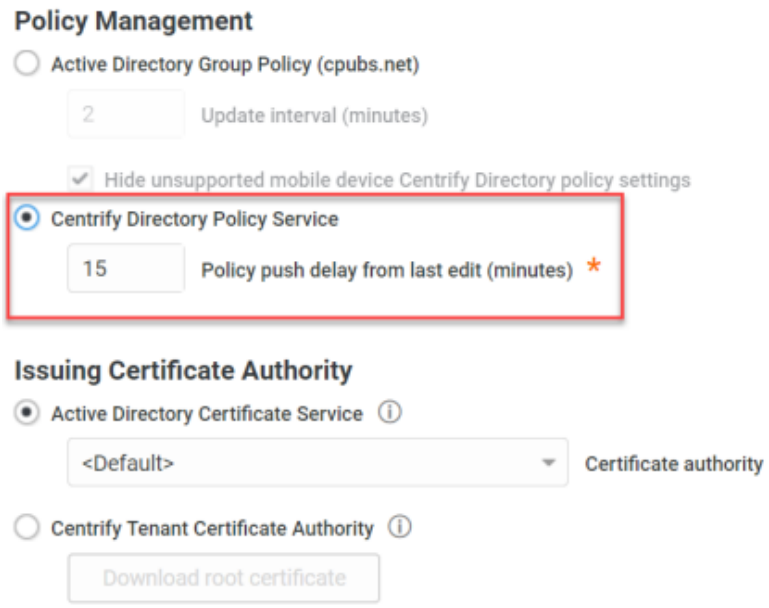
Selecting the Centrify directory policy service

If you select Centrify directory policy service, the Privileged Access Service uses the policy sets assigned to each role to set the device configuration policies.

Click the **Download** button to download the certificate for the Centrify CA for your account for installation in the Exchange server, wi-fi access point, or VPN server or concentrator. The certificate is self-signed.

To select Centrify directory policy service for device policy management:

1. Log in to Admin Portal.
2. Click **Settings > Endpoints > Endpoint Management Settings**.
3. Enable **Centrify Directory Policy Service**.



4. Click the text box and enter the number of minutes for **Policy push delay from last edit**.

   The policy push delay specifies the number of minutes Privileged Access Service waits from the time you saved the policy set to push the changes to the devices.

5. Select the issuing certificate authority.

   You can use either the Active Directory Certificate Service or the Centrify Certificate Authority (CA) to generate user and computer certificates to authenticate users and devices for wi-fi connections, respectively. The certificates are created and installed on the device when the user registers the device. The default selection is Active Directory Certificate Service.

   a. Select **Active Directory Certificate Service** to use the default certification authority you configured in your Active Directory Certificate Service. (You can only use the default certification authority.) If you select this option, you need to create user and computer templates on the default certification authority. There may be some additional configuration required in the connector as well. See How to use Active Directory certificates in devices for authentication for the details.

   b. Select **Centrify Tenant Certificate Authority** to use the Centrify CA for your Privileged Access Service account to generate user and computer certificates instead. You do not need to create templates when you select this option.

      Privileged Access Service includes a self-signed Centrify CA for each customer Privileged Access Service. When you select the certification authority, it generates certificates that can be used to authenticate users for wi-fi and VPN connections and ActiveSync server log ins (Exchange 2010 and older only). The certificates are automatically generated and installed for users who are a member of a role that has a wi-fi, VPN, or Exchange server profile in the Centrify directory policy service in which certificates are used for authentication. The certificates are installed automatically when users register their devices.

   c. (Optional) Click the **Download root certificate** button to download the certificate for the Centrify CA to install in the Exchange server (2010 and older), wi-fi access point, or VPN server or concentrator.

6. Click **Save**.

Selecting Active Directory Group Policy

If you select Active Directory group policy, the Privileged Access Service uses the group policy object you linked to the organizational unit specified in the Device Registration Settings for each role to set the device configuration policies.

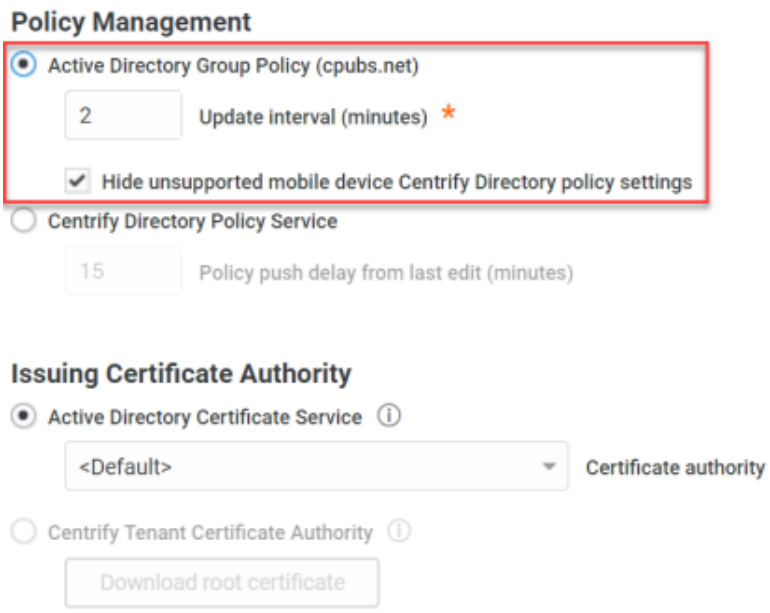
The certification authority you select generates certificates that can be used to authenticate users for wi-fi and VPN connections and Exchange ActiveSync server log ins. The certificates are automatically generated and installed for users who are a member of a role that has a wi-fi, VPN, or Exchange server profile in the group policy object linked to their organizational unit. The certificates are installed automatically when the user registers the device.

When you install the connector, it searches the Active Directory forest for the certification authorities you have configured in your Active Directory Certificate Service. You can select any certificate authority it finds to generate certificates.

Note: When you use an Active Directory certification authority, you need to create user and computer templates on the certification authority you select. There may be some additional configuration required in the connector as well. See How to use Active Directory certificates in devices for authentication for the details.

To select Active Directory for device policy management:

1. Log in to Admin Portal.
2. Click **Settings > Endpoints > Endpoint Management Settings**.
3. Enable **Active Directory group policy** in the Policy Management area.



4. Set the update interval.

   The update interval sets how often the Privileged Access Service polls the domain controller for changes to the group policy objects. If the Privileged Access Service finds a group policy object has changed, it pushes the policy changes to the devices. Otherwise, it takes no action.
5. Configure **Hide unsupported mobile device Centrify Directory policy settings**. Enabled by default.

Some device configuration policy settings are available for both Active Directory users policy settings managed using Windows Group Policy Management Editor (GPME)) and Centrify Directory users (policy settings managed using Admin Portal), while some are only available in Admin Portal for managing Centrify Directory users. When **Hide unsupported mobile device Centrify Directory policy settings** is enabled, we hide those device configuration policy settings that are only available in Admin Portal to minimize confusion.

Typically, you disable this setting when your are planning to migrate your Active Directory users to Centrify Directory, so you can see all the device configuration policy settings and make the necessary configurations.

6. Configure the issuing certificate authority.

   Selecting **Active Directory group policy** automatically assigns the Active Directory Certificate Service as the issuing certificate authority.

   If you do not want to use the default certification authority, use the drop-down menu to select another. When you install the connector, it searches the Active Directory forest for the certification authorities you have configured in your Active Directory Certificate Service. You can select any certificate authority it finds to generate certificates.

   The certification authority you select generates certificates that can be used to authenticate users for wi-fi and VPN connections and Exchange ActiveSync server log ins. The certificates are automatically generated and installed for users who are a member of a role that has a wi-fi, VPN, or Exchange server profile in the group policy object linked to their organizational unit. The certificates are installed automatically when the user registers the device.

   Note: When you use an Active Directory certification authority, you need to create user and computer templates on the certification authority you select. There may be some additional configuration required in the connector as well. See How to use Active Directory certificates in devices for authentication for the details.

7. Click **Save**.

Configuring Group Policy Objects and Organizational Units

When you use Active Directory group policy to set device configuration policies, you use group policy objects that you edit with the Group Policy Management Editor to set the policies. Next, you link that group policy object to an organizational unit. Finally, you specify the organizational unit to use for a given policy set when you configure the Device Registration Settings (see How to register devices).

The organizational unit you specify in the Device Registration Settings is also the organizational unit in which the Privileged Access Service stores the Active Directory record when the user registers the device. You can use this record in Active Directory Users and Computers to get information about the device and send it commands. See Using Active Directory Users and Computers to manage devices for the details.

When you select Active Directory group policy, you should plan on how you will apply the group policy objects to Privileged Access Service roles before you create the policy sets and assign them to the roles. When you have your roles and policies planned, you use the following procedure to apply them to individual devices:

1. Create a separate organizational unit for each role.
2. Create the group policy object for that role and set the policies.
3. Link the group policy object to the organizational unit.

4. Specify the organizational unit when you set the Device Registration Settings for the policy set (see How to register devices).
5. Assign the policy set to the role.
6. Add the users to the role.

You can use multiple roles or policy sets to apply different policies to users. In this case the rules for hierarchical policies are applied "Using Hierarchical Policy Sets" on page 722.

Policy Summary

For users and resources, the summary shows the summation of all policies applied and the name of the policy set applying the policy. By default, the summary for an individual resource is for the logged-in user viewing the summary as shown in the selected user field at the top of the screen.

Assigning Permissions

Administrative rights and permissions control what different users see and can do with the applications, systems, domains, databases, secrets, services, accounts, and sets stored in the Privileged Access Service. You can assign and manage different permissions based on the type of object you have selected. For example, the permissions available for managing systems or applications are different from the permissions available for managing databases or when working with sets of those objects. In addition, the specific permissions available for you to assign and the specific activities those permissions control depend on the permissions you have, the type of object you are managing, and the scope for where the permission applies.

You can assign different levels of permissions:

- Permissions that are specific for **individual** resources and applications.
- Permissions that apply to **logical sets** of resources and applications.
- Permissions that apply **globally** for specific accounts and systems.

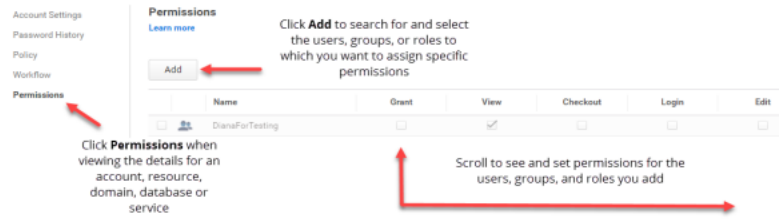
See "Common Permissions" on page 745 and the "Additional Account Permissions" on page 748 topics in this section for more information.

Navigating to Permissions

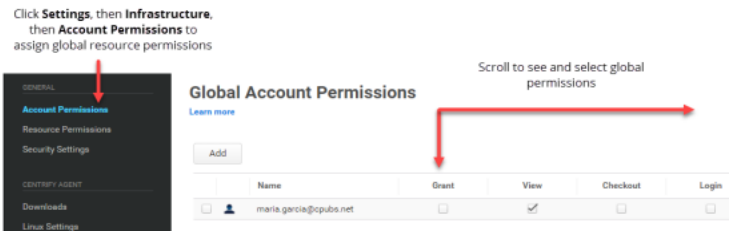
There are several paths you might take to get to where permissions are assigned for any given object, but the most common path is through the permissions page of the object details:

- Permissions for specific objects (for example; applications, systems, domains, databases, services, and accounts) are assigned when viewing the details for the individual object.
- Permissions for sets of objects–and the set members, if the set membership is manually defined–are assigned when viewing the details for the set.

For example, if you are viewing the details for a specific account, you would click **Permissions**.



You can also define global permissions to set default permissions on all accounts or on all systems for selected users, groups, or roles. Global permissions are defined on the **Access** tab under **Global Account Permissions**.



Administrative Rights and Permissions

Individual permissions enable you to manually set granular rights on applications, systems, domains, databases, secrets, services, and accounts. You can also assign permissions automatically through administrative rights and roles. By creating roles with specific administrative rights, you can customize the user experience for people who need to perform different tasks. For information about adding roles and adding administrative rights to a role, see "Admin Portal Administrative Rights" on page 277.

Inherited Permissions

Permissions can be inherited from global settings or from administrative rights granted using Privileged Access Service roles. When you are viewing or setting permissions, the **Inherited From** column indicates whether

the permission settings were inherited or explicitly granted for each user, group, or role listed. The **Inherited From** column is blank for users who are explicitly granted permissions. Permissions set by inheritance cannot be modified directly.

Viewing Temporary Permissions

If you have configured a “request and approval” work flow for an account, some users might have temporary Login or Checkout permissions. If any of the permissions are temporary because a request for access has been approved, the **Expires** column indicates when the permission will expire.

If an access request is approved and set to expire, active sessions can continue past the expiration. However, users will not be allowed to log on or check out a password without submitting a new request for access.

Only users who have requested and been granted temporary access by a designated approver display an expiration. The **Expires** column is blank for users who are explicitly granted a permission outside of the “request and approval” work flow. For more information about enabling a “request and approval” work flow, see "Request and Approval Workflow Overview" on page 774.

Common Permissions

The Grant, View, Edit, and Delete permissions are the most commonly available permissions for different types of objects. All of the common permissions are supported for sets of objects as well as systems, domains, databases, and their associated accounts.

Only Grant, Edit, and Delete permissions are supported for services and multiplexed accounts.

Only Grant and View are available for applications.

Grant

Select **Grant** to allow users to grant any permissions to other users for applications, systems, domains, databases, services, or accounts. By default, members of the System Administrator role have Grant permissions for all objects. In addition, users who add objects to the Privileged Access Service have the Grant permission on the objects they add.

Users who are assigned the Grant permission on a set, however, can only assign permissions they have on the members of the set. For example:

- If you have the Grant permission on a set that includes two computers, you can only grant other users the Manage Session permission if you have the Manage Session permission on both computers in the set.
- If you only have the Checkout permission on the members of the set, you cannot grant other users permissions such as Login or Update Password.
- If you only have the View permission on members of an applications set, you cannot grant other members the Run permission.

View

Select **View** to allow users to view applications, systems, domains, databases, secrets, services, or accounts. A user, group, or role must be assigned the View permission to take any kind of action.

If you store text strings or files as secrets, however, the View permission also allows users to view stored text or download stored documents.

Edit

Select **Edit** to allow users to edit information for systems, domains, databases, secrets services, or accounts.

- The specific information available to be edited depends on whether you have selected a system, domain, database, secret, service, account, or set of objects. For example, you must have the Edit permission to select the **Manage this credential** option or to update any optional description.
- If you store text strings or files as secrets, however, the Edit permission also allows users to edit stored text or replace stored documents.

Delete

Select **Delete** to allow users to delete systems, domains, databases, services, or accounts.

You should note, however, that assigning the Delete permission is not always sufficient to enable users to delete objects. For example, deleting a system from the Privileged Access Service requires you to first delete all of the accounts that have been stored for that system. A user with the Delete permission on a system but not on the accounts for the system would be prevented from deleting the system until someone with the Delete permission for the accounts removed all of the accounts stored for the system.

Users who have Delete permission for accounts must also have Checkout permission because before deleting an account you must display or copy the password to prevent the account from being unusable.

Additional System Permissions

There are a few permissions that are unique to systems. These permissions can be set for individual systems, sets of systems, or globally for all systems.

If you are working with systems, you can set the following additional permissions:

- Select **Manage Session** to allow users to watch or terminate active sessions on systems.
- Select **Agent Auth** to allow users to authenticate and log on to systems where the Delinea Client is installed. The **Agent Auth** permission enables users who have an account on the Privileged Access Service to log on to a registered Linux or Windows computer. For example, if your organization uses Privileged Access Service, you might have user account defined for each

employee or for employees in specific roles. You can enable all employees or employees in the selected roles to log on to the Admin Portal using their Privileged Access Service user account and to use that same account to log on to registered Linux or Windows computers if they are granted the **Agent Auth** permission on that registered Linux or Windows computer.

- Select **Request Zone Role** to allow users to request access to a collection of rights for computers in a zone. The **Request Zone Role** permission allows a user to request assignment of a particular Privileged Access Service zone role to use the elevated privileges associated with the role on the computers in a domain or zone.This permission requires several preliminary steps to be completed. For example, you must enable the zone role workflow for the domain and configure the list of zone roles that can be requested by a user, the system must be joined to a zone, and the requesting user must be an Active Directory user. For more details about the preliminary steps for using this feature and permission, see Managing zone role assignment requests and related topics. For an introduction to rights and roles, role assignments that do not use a request and approval workflow, and managing privilege elevation for computers in zones, see Welcome to Server Suite.
- Select **Add Account** to allow a user to add Privileged Access Service accounts to a system. If this system permission is not selected, attempting to add a new account to a system will fail.
- Select **Unlock Account** to allow accounts (used to access a system) the permission to manually unlock managed local accounts. This permission only applies to systems with the correct policies in place for local account password reconciliation. See "Configuring Domains for Local Account Password Reconciliation" on page 549.

Additional Domain Permissions

There are a few permissions that are unique to domains. These permissions can be set for individual domains or sets of domains.

If you are working with domains, you can set the following additional permissions:

- Select **Unlock Account** to allow accounts used to access a domain permission to manually unlock managed domain accounts.
- Select **Add Account** to allow a user to add Privileged Access Service

domain accounts. If this domain permission is not selected, attempting to add a new account will fail.

For more information about working with domains and adding and unlocking accounts, see "Managing Domains" on page 671 and "Setting Domain-specific Policies" on page 491.

Additional Secret Permissions

There is one permission unique to secrets. This permission can be set for individual secrets or sets of secrets.

If you are working with secrets, you can set the following additional permission:

- Select **Retrieve Secret** to allow users to retrieve secret text strings, stored files, or passwords associated with stored files.

For more information about working with secrets, see "Managing Secrets" on page 677.

- Select **Request CSS Role** to allow users to authenticate and log on to all resources where the Server Suite Agent is installed.

Additional Account Permissions

There are several additional permissions that are unique to accounts. These permissions can be set for individual accounts, sets of accounts, or globally for all accounts.

The account permissions available depend on the type of account you have selected:

- Local accounts support all of the common and account permissions.
- Domain and database accounts support all of the common and account permissions except the Login and Workspace Login permissions.
- Multiplexed accounts only support the Grant, Edit, and Delete permissions and require additional permissions for systems.

Checkout

Select **Checkout** to allow users, groups, or roles to display or copy the password for a selected account.

If the password for the account is managed by the Privileged Access Service, this permission also results in the generation of a new password when the password is checked in manually or when the checkout period expires. If the password is not managed by the Privileged Access Service, this permission enables users, groups, or roles to display or copy a password that will remain unchanged until manually updated.

Login

Select **Login** to allow users, groups, or roles to log on to a target system or domain using a secure shell (ssh) session or remote desktop (rdp) connection in a web browser or with a native local client.

The Login permission enables users, groups, or roles to log on without knowing the account password. Because the password is not displayed, this permission enables secure access to remote systems and domains when using managed or unmanaged accounts.

File Transfer

Select **File Transfer** to allow users, groups, or roles to securely transfer files using secure copy (scp) or secure file transfer (sftp) while logged on remotely to a target computer. Users who have the File Transfer permission but don't have Login permission for the target computer can request access if a request and approval workflow is enabled. Only users who have the File Transfer permission can use accounts in the Privileged Access Service to perform file transfer operations.

Update Password

Select **Update Password** to allow users, groups, or roles to update the password for a selected account. The Update Password action is available for both managed and unmanaged accounts you add to the service. In both cases, be sure you have the correct current password for the account. If you are unsure, reset the password on the target system first, then update the password stored in the privilege service.

Workspace Login

Select **Workspace Login** to allow users, groups, or roles to log on to a system using the selected account and stored password. The account is added to the "My System Accounts" table on the **Workspace** page. You do not need any particular role assignment to use this permission.

Rotate

Select **Rotate** to allow users, groups, or roles to change the password stored in the Privileged Access Service for a managed account immediately without waiting for the rotation period to expire.

This permission enables selected users to rotate the password "on demand" if there has been suspicious activity or a risk that the password has been compromised.

Additional Application Permissions

In addition to the Common permissions that are applicable to applications and application sets, the following permissions are specific to application objects.

Permission	Description
Manage	Provides get Read, Write, and Delete permission to applications and sets of applications.
Run	Allows users to launch the application.

Configuring Global Settings

You can use the Settings for Privileged Access Service to configure global defaults and options, such as the permissions granted for accounts and systems, built-in and custom password complexity rules you want to use, and preferences for remote client connections. In most cases, you can override these global settings for individual systems, domains, databases, or accounts, where needed. The global settings only apply where you have not explicitly configured a setting for an individual system, domain, database, or account.

Setting Global Account Permissions

You can use global account permissions to define the specific permissions granted to different users when they use the accounts stored in the Privileged Access Service. The global account permissions apply to all systems, domains, or databases you add by default. You can also override the default permission for individual systems, domains, or databases, as needed.

Most of the activity in the Admin Portal involves managing systems, domains, and databases and the accounts that are specifically used to access them. For example, when you manage user permissions for an account on a particular server, those permissions only apply in the context of that particular account on that specific server.

In some cases, however, you might want to define global account permissions that apply for all systems instead of system-specific permissions. For example, you might want to define a global account permission that allows the admin1@pubs.org user to log on without a password to all target systems you add to the Privileged Access Service, then grant that user the permission to check out an account password only for a specific system and account combination. Similarly, you can grant global account permissions for domains and databases.

The Login and Checkout permissions configured in the global or sets account permissions directly map to the Login and Checkout permission for the account for most accounts (e.g. local accounts, domain accounts, etc). There are two exceptions:

- For IAM User accounts:
  - Login permission maps to the Use Access Key permission
  - Checkout permission maps to the Retrieve permission.
- For IAM Role accounts, the Login permission maps to the Assume Role permission.

To Set the Global Account Permissions

1. In the Admin Portal, click **Settings** > **Resources** > **Security** > **Global Account Permissions**.
2. Click **Add** to search for and select users, groups, roles, or computers.
   - Type a search string to search for the users, groups, or roles to which you want to grant global permissions.
   - Select the appropriate users, groups, or roles from the search results.
   - Click **Add**.
3. Select the appropriate global account permissions for each user.

   As an administrator in the System Administrator role, your user account has all permissions by default. You can assign specific global rights to otherusers to allow them to work with accounts on all managed systems. Note thatusers must have both the Delete and Checkout permission to delete accountsbecause you must be able to display or copy the password for an accountbefore deleting it. For more detailed information about the permissions available, see "Assigning Permissions" on page 743.

   If any of the permissions are temporary because a request for access has been approved, the **Expires** column indicates when the permission will expire.
4. Click **Save** to save the global account permissions settings.

Viewing Temporary Permissions for Users

If you have configured a “request and approval” work flow for an account, some users might have temporary Login or Checkout permissions. If a request for login or password checkout has been temporarily approved, the permission will have an expiration date and time. Active sessions can continue past the expiration, but users will not be allowed to log on or check out a password without submitting a new request for access.

Only users who have requested and been granted temporary access by a designated approver display an expiration. The Expires column is blank for users who are explicitly granted a permission outside of the “request and approval” work flow or granted a permanent permission by a designated approver.

Configuring Password Profiles

You can use global **Password Profiles** to define the rules applied when managed passwords are generated. There are default predefined profiles for the different types of accounts used to access systems, domains, and databases. You can clone and modify the default profiles or add your own custom profiles. You can also override the default profile for individual systems, domains, or databases, as needed.

Password profiles specify details such as the minimum and maximum number of characters the password should contain, whether lower or upper case letters are required, and which special characters are allowed. The rules you define in any custom profile should reflect what is supported in a specific type of environment. For example, some HP-UX computers don't allow passwords to contain @ or # characters.

The default set of password profiles are assigned based on the underlying operating system, such as UNIX, Windows, or Cisco NX-OS or the database type, such as Oracle or SQL Server. See the following for a complete list of supported environments and additional details:

- "Managing Systems" on page 687
- "Managing Domains" on page 671

- "Managing Databases" on page 660

You can change the default assignment for any specific system, domain, or database.

Only members of the System Administrator role can add, edit, clone, or delete password profiles. Members of the Privilege Service Administrator role can change the profile for any specific system, domain, or database. Members of the Privilege Service Power User role can only view the global profile settings.

To Configure a New Password Profile

1. In the Admin Portal, click **Settings >Resources** to display the settings available for Privileged Access Service.
2. Click **Password Profiles**.
3. Click **Add** to create a new custom password profile.

   Alternatively, you can select any existing profile, right-click, then click **Clone Profile** to create a new custom password profile.
4. Type a profile name and optional description.
5. Set the minimum and maximum password length.

   These settings allow randomly-generated passwords to vary in length. Before setting these values, however, you should consider whether there arepassword limitation that are specific to the operating system, domain, or database where the profile will be used.
6. Set any additional password complexity requirements as appropriate for the operating system, domain, or database where the profile will be used.
7. Click **Save** to save the password profile.

Setting Global System Permissions

You can use system-specific or global system permissions to define the specific permissions granted to different users when they use the accounts stored in Privileged Access Service. The global permissions apply to all systems you add by default.

To Set the Global System Permissions

1. In the Admin Portal, click **Settings** > **Resources** > **Security** > **Global System Permissions**.
2. Click **Add** to search for and select users, groups, or roles.
   - Type a search string to search for the users, groups, or roles to which you want to grant global system permissions.
   - Select the appropriate users, groups, or roles from the search results.
   - Click **Add**.
3. Select the appropriate global system permissions for each user, group, or role.

   For more detailed information about the permissions available and the permissions that are specifically for systems, see "Assigning Permissions" on page 743.
4. Click **Save** to save the global system permissions settings.

Setting Global Security Options

As a user with the System Administrator role, you can set security and maintenance options that apply globally to the all of the systems, domains, or databases you add to the Privileged Access Service. Most of these settings are the same as described in the following topics:

- "Setting System-specific Policies" on page 556
- "Setting System-specific Advanced Options" on page 561
- "Setting Domain-specific Advanced Options" on page 488
- "Setting Database-specific Advanced Options" on page 662

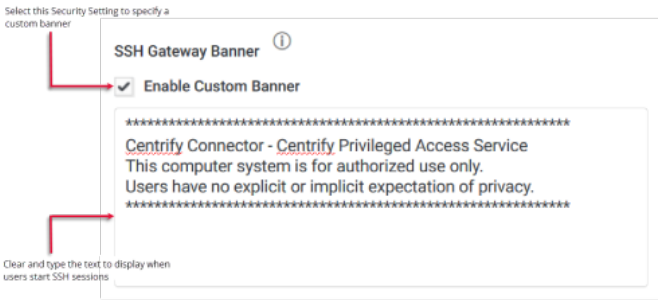
After you set a global security option, that setting becomes the default used for all systems, domains, and databases unless you explicitly set a system-specific, domain-specific, or database-specific option to override it.

Fore more information about global security options that cannot be set for individual systems, domains, or databases, see:

- "Updating the SSH Gateway Banner" below
- "Downloading the SSH Master Key File" on page 86
- "Password Profiles" on the next page
- "Allow Permanent workflow requests for password checkouts" on page 755
- "Allow Permanent Workflow Requests for Login" on page 755
- "Enable Periodic SSH Key Cleanup at Specified Interval (days)" on page 755
- "Enable Periodic SSH Key Cleanup at Specified Interval (days)" on page 755
- "Require Secure Communication Method for Remote (RDP) Connections" on page 755
- "Viewing All System Admin Sets" on page 686
- "Configuring Cloud Directory Lookup Priority" on page 755

Updating the SSH Gateway Banner

If you enable SSH gateway for a connector, remote sessions display a default welcome message to authorized users when they log on using a native SSH client. You can review or modify the message displayed by selecting **Settings > Resources** > **Security Settings** and selecting the **Enable Custom Banner** option.



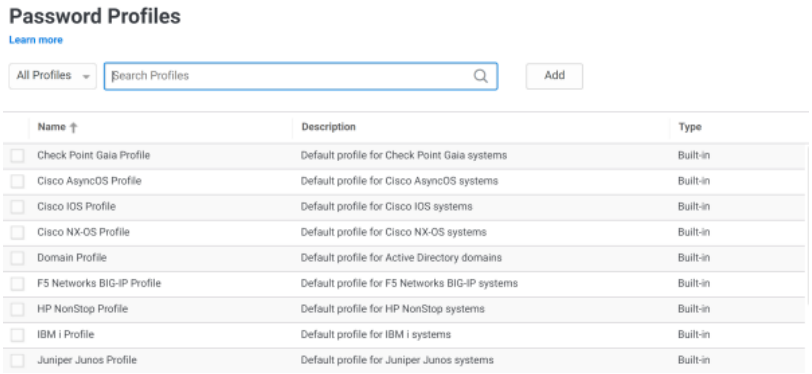
If you disable the SSH gateway for a connector, the message is not displayed.

To restore the default gateway banner, select **Resources**> **Security Settings** > **Enable Custom Banner**, then remove the custom banner text.

For more information about using remote client programs to connect to target systems, domains, or databases, see Configuring remote client operations and settings.

Password Profiles

In addition, you can use the global security settings to identify the default password complexity profile you want to use or create a new one for each type of system, domain, or database account you add to the Privileged Access Service. For example:



The default password profile provided for each type of system, domain, or database will only include the appropriate supported special characters. If you clone a profile or change the profile mapping to create custom password profiles, you should be aware that some special characters might not be supported on a given system, domain, or database and should not be used in the password.

To Set Global Security Options

1. In the Admin Portal, click **Settings**, then click **Resources** to display the settings available for Privileged Access Service.
2. Click **Security Settings**.

3. Select the specific policies you want to use as global policies.

   For more information about these policies, see the information pop-up help or the descriptions of the advanced options for systems, domains, or databases.

4. Click **Save**.

Allow Permanent workflow requests for password checkouts

Uncheck to disable or check to enable the ability to request permanent permission for the user to check out a password.

Allow Permanent Workflow Requests for Login

Uncheck to disable or check to enable the ability to request permanent permission for the user to login.

Enable Periodic SSH Key Cleanup at Specified Interval (days)

Specifies whether retired SSH keys should be deleted periodically. Uncheck to disable or check to enable the ability to allow periodic SSH key cleanup.

Enable Periodic SSH Key Rotation at Specified Interval (days)

Specifies whether managed SSH key should be rotated periodically. Uncheck to disable or check to enable the ability to allow periodic SSH key rotation. Leave unchecked to not allow periodic SSH key rotation.

Require Secure Communication Method for Remote (RDP) Connections

Check or enable to require SSL or client negotiation to secure communication between clients and RD session host servers. Native RDP encryption may be used for communications between the client and RD Session Host server when client negotiated. The RD Session Host server is not authenticated when this occurs.

Note: We do not recommended disabling this function.

Configuring Cloud Directory Lookup Priority

For Windows systems that are joined to Active Directory and have the Delinea Client installed, you can make sure that the service looks for UPNs in the cloud directory only by specifying a comma-separated list of domain suffixes in the field entitled as follows: **Use the cloud directory to look for users based on UPNs that match the following domain suffixes (Windows only)**. This setting is available in **Settings > Resources > Security > Security Settings**.

If this list is empty or a UPN suffix doesn't match any suffixes in this list, the service looks for the UPN in Active Directory first; if the user isn't in Active Directory, the service then looks for the UPN in the cloud directory.

For example, if the affected uses are alex@acme.com and joe@foo.com, then you would enter "acme.com, foo.com" in this field.

Configuring Password Storage

By default, the passwords for the accounts you add to the Privileged Access Service are stored securely in the Privileged Access Service. If you prefer to store them in a key management appliance or hardware security module

appliance–such as an on-site SafeNet KeySecure appliance–you can configure the Privileged Access Service to store and retrieve system passwords using the supported external appliance.

Note that you must have the SafeNet KeySecure appliance installed and configured and available on the network before configuring it for the storage of Privileged Access Service passwords. You can use client certificates created by the Delinea service or a client certificate you have created on your own.

To Store Passwords in SafeNet KeySecure

1. In the Admin Portal, click **Settings**, then click **Resources** to display the settings available for Privileged Access Service.
2. Click **Password Storage**.

   If you have not yet configured secure communication between the Connector and the SafeNet KeySecure appliance, click **Configure settings for SafeNet KeySecure** to open global settings in the administrative portal for the Privileged Access Service. For more information about configuringSafeNet KeySecure to store passwords for Privileged Access Service accounts, see "Managing Password Storage" below.
3. Select the location for storing passwords.

   For example, select **SafeNet KeySecure appliance** to store passwords in a SafeNet KeySecure appliance.
4. Click **Save** to save the password storage location.

   Saving a new password storage location will prompt you to migrate passwords to the new location immediately. Click **Yes** to migrate all existingpasswords. If you click No, only new passwords are stored in the newlocation. If you click No, you can click **Migrate Passwords** at a later time to migrate previously stored passwords to the new location.
5. Specify the email address where you want to receive notification of the migration results, then click **Yes**.

For more information about checking password migration status, see the following topics:

- "Viewing Migration Status" on page 758
- "Notification if Managing the Service On-site" on page 758

Managing Password Storage

By default, the passwords for the accounts you add to the Privileged Access Service are stored securely in a local repository if you are managing the service on your own network or in the Privileged Access Service if you are using the cloud-based service. If you prefer to store them in a key management or hardware security appliance such as an on-site or off-site SafeNet KeySecure appliance, you can configure the Privileged Access Service to store and retrieve account passwords using the supported external appliance.

For more information about managing account passwords using a key management appliance such as SafeNet KeySecure, see the following topics:

- "To Store Passwords in SafeNet KeySecure" above
- "Installing and Configuring SafeNet KeySecure" on page 768
- "To Configure Communication Between with SafeNet KeySecure" on the next page
- "To Store Passwords in SafeNet KeySecure" above

Configuring Communication with SafeNet KeySecure

If you want to use a SafeNet KeySecure appliance to store account passwords, you first must configure secure communication between the appliance and the Connector. Because this is a global setting, it is configured in the Admin Portal for the Privileged Access Service and requires you to have an account in the System Administrator role.

To Configure Communication Between with SafeNet KeySecure

1. Select **Switch to Admin Portal** from the account name menu.
2. Click the **Settings** tab.
3. Select **Resources** from the list of setting categories, then select **SafeNet KeySecure Configuration**.
4. Type the IP address or the fully-qualified domain name of the key management appliance and specify the port number you configured for the key server instance.

   If you have SafeNet KeySecure running on a cluster, you can specify multiple IP addresses separated by colons (:). For example, if configuringcommunication for a cluster, you would specify a list of IP addresses using a format similar to this:

   192.168.1.1**:**192.168.1.1**:**192.168.1.3

   This example specifies the IP addresses for appliances in a single tier. For more information about working with KeySecure appliances in clusters and specifying multiple tiers, see Working with appliances in a cluster.
5. Click **Upload** to navigate to the SafeNet KeySecure Root CA certificate that you downloaded from the KeySecure appliance.
6. Select the client certificate-issuing authority.

   If you select the Delinea-issued certificate, click **Download** to download the Delinea CA certificate that will make the Delinea-issuedcertificate trusted by the SafeNet KeySecure appliance. After downloadingthe certificate, you can use the SafeNet KeySecure management console toinstall the certificate on the appliance. For more information aboutinstalling the Delinea-issued certificate, see Install the client certificate.

   If you select Customer-issued certificate to use the client certificate you created in the KeySecure management console or using another tool, click**Upload**. You can then navigate to and select the client certificate that you want to use for the Connector.

   Uploading a client certificate you created will prompt you for a password. If the client certificate requires a password to authenticate, type thepassword then click **Continue**. If no password is required, simply click**Continue** without specifying a password.
7. Click **Save** to save the configuration settings.

After you have saved the configuration–including uploading or downloading and installing the client certificate–you can verify communication between the Privileged Access Service and the SafeNet KeySecure appliance. However, the option to test the connection is only available after you complete the configuration.

For complete information about installing and configuring a SafeNet KeySecure key management appliance, see the *KeySecure Installation and Configuration Guide*.

Viewing Migration Status

After you start the job, you can view the status and results of the job by clicking **View Migration Job Status and Reports** or wait to receive email notification that migration is complete. The email notification will provide a link to the job history. You can then click the link in the email to see details about the migration results. Because the job history report can list details for different types of jobs, you can use the Search field to filter the jobs displayed.

For complete information about installing and configuring a SafeNet KeySecure hardware appliance, set the *KeySecure Installation and Configuration Guide* and "Managing Password Storage" on page 756.

Notification if Managing the Service On-site

If you have installed Privileged Access Service on your internal network and are managing the service yourself, you must configure the settings for a custom Simple Mail Transport Protocol (SMTP) mail server in the administrative portal to receive email notification about the results of password migration jobs. For details about post-installation configuration steps when you deploy Privileged Access Service as an on-site service, see the *Installation and Configuration Guide for On-Site Deployment*.

Configuring Global Account Workflow

To simplify the process of configuring a “request and approval” workflow for privileged accounts, you can enable workflow as a feature that applies to all accounts stored in the Privileged Access Service. You can then select a single user or role to approve all login and password checkout requests. You can also use this global setting in conjunction with account-specific settings to selective restrict access requests for some accounts or modify the user or role with approval authority.

To Configure Workflow for All Accounts

1. In the Admin Portal, click **Settings**, then click **Resources** to display the settings available for the Privileged Access Service.
2. Click **Global Account Workflow**.
3. Select **Enable Workflow for all accounts**.
4. Click **Select** and type a search string to search for and select a user or role with authority to approve login and password checkout requests, then click **Add**.
5. Click **Save**.

After you have configured the workflow for all accounts, users with Privilege Service Power User rights can request login and password checkout access for the accounts stored in the Privileged Access Service. You can use

account-specific settings to override the global workflow. For example, you can use account-specific settings to prevent access requests for some accounts or to modify the user or role with approval authority.

Configuring Global Agent Auth Workflow

To simplify the process of providing Agent Auth workflow for systems, you can enable Agent Auth workflow as a feature that applies to all systems in Privileged Access Service. You can use system-specific settings to override the global workflow. For example, you can use system-specific settings to prevent access requests for some systems or to modify the user or role with approval authority.

To Enable Workflow for All Systems

1. In the Admin Portal, click **Settings**, then click **Resources** to display the settings available for the Privileged Access Service.
2. Click **Global Login Workflow**.
3. Select **Enable Workflow for all Systems**.
4. From the **Approver List**, select either **Requestor'sManager** or **Specified User or Role**.

   Note: If using Requestor's Manager approver, and the requestor has no manager, you can select automatically approve, deny, or route to another user/role.

5. Click **Add** and select user and role.
6. Once added, click **Save**.

For more information on using Agent Auth workflow, see "Using Agent Auth Workflow" on page 801

Configuring Global Secret Workflow

To simplify the process of providing retrieve secrets workflow for secrets, you can enable secrets workflow as a feature that applies to all secrets stored in the Privileged Access Service. You can also use this global setting in conjunction with secret-specific settings to restrict access requests for some secrets or modify the user or role with approval authority.

To Configure Workflow for All Secrets

1. In the Admin Portal, click **Settings**, then click **Resources** to display the settings available for the Privileged Access Service.
2. Click **Secrets Workflow**.
3. Select **Enable Workflow for all Secrets**.
4. From the **Approver List**, select either **Requestor'sManager** or **Specified User or Role**.

   Note: If using Requestor's Manager approver, and the requestor has no manager, you can select automatically approve, deny, or route to another user/role.

5. Click **Add** and select user and role.
6. Once added, click **Save**.

After you have configured the workflow for all secrets, users with Privilege Service Power User rights can request retrieve access for the secrets stored in the Privileged Access Service. You can use secret-specific settings to override the global workflow. For example, you can use secret-specific settings to prevent secret retrieve requests for some secrets.

Mapping System Subnets to Connectors

By default, systems use any available connector without evaluating the network topology. If the communication with a current connector is interrupted, systems automatically select another available connector to continue operation. As a user in the System Administrator role, however, you can assign the specific connectors that should serve a specific logical group of systems by mapping a subnet pattern to a selected set of connectors. Systems matching the subnet pattern will use the specific connectors you select for them.

By mapping system subnets to specific connectors, you can also control overall load balancing and failover. You can override the global rules for system subnet mapping for individual systems. System-specific settings take precedence over global connector subnet mapping. In addition, more restrictive subnet mapping takes precedence over less restrictive mapping.

> **Note:** PAS does not use subnet mapping to restrict which connector can be used as a jumpbox. Subnet mapping only tells PAS which preferred connector(s) to use when you are trying to access a remote system or perform account password management operations on a system.

If you don't map system subnets, understand that the client prioritizes connectors in the following order:

1. Connectors in the same subnet and same site as the client computer
2. Connectors in the same site as the client computer
3. Connectors that are in a different site from where the client computer is
4. Any remaining connectors

See Configuring template mappings for information about how to configure system resource mappings for your connector.

To Map System Subnets to Connectors

1. In the Admin Portal, click **Settings >Resources** to display the settings available for Privileged Access Service.
2. Click **System Subnet Mapping**.
3. Click **Add**.
4. Type the subnet for a group of systems using Classless InterDomain Routing (CIDR) notation, for example, 192.168.1.0/24.

   Keep in mind that a more restrictive subnet pattern takes precedence over a less restrictive pattern if the rules you define result in overlapping system subnet matches.
5. Click **Choose** and select the specific connectors you want to use for systems in the specified subnet.

   Alternatively, you can select **Any available** if you want to allow any connector available on your network for systems in the specified subnet.
6. Click **Done** to save the subnet to connector mapping.

Adding Systems Using Enrollment Codes

If you want to automate the process of adding new systems to the Privileged Access Service, you can do so by creating and using a randomly-generated enrollment code. Enrollment codes enable you to automatically join multiple computers matching certain criteria to the Privileged Access Service without specifying user credentials. Without an enrollment code, adding new computers would require you to provide credentials to verify that you have permission to perform the operation or hard-coding a user name and password in an enrollment automation script.

To Automate Enrollment and Avoid Storing any User Names or Passwords

in automation scripts, you can create one or more enrollment codes that specify a domain pattern to identify the computers you want to add. You can also specify how many times the code can be used, that is, the maximum number of computers the code can be used to add, and when the enrollment code should expire.

Some things to remember about enrollment and enrollment codes:

- Enrollment codes can only be used to add computers to the Privileged Access Service and don't provide access to any sensitive information or grant any elevated privileges.
- You must be a member of the System Administrator role to generate enrollment codes.
- You must be in a role with the System Enrollment administrative right to add computers to the Privileged Access Service when using a user name and password.
- You can use an enrollment code to add the computer without supplying a user name and password.

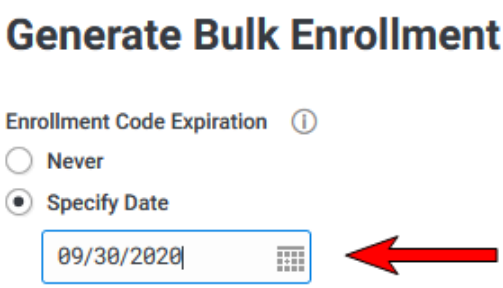
In most cases, adding a computer to the Privileged Access Service makes you the owner of the computer object with permission to delete the computer account and the ability to delegate permissions to other users. However, if you add computers using an enrollment code, the built-in SYSTEM account becomes the owner of the computer object. Only members of the System Administrator role can grant permissions on computers owned by the SYSTEM account.

For more information about running the cenroll command and other command-line programs, see the Linux man pages or Windows command-line help installed with the software.

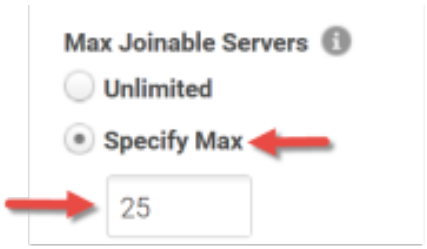
To Automate the Process of Adding Computers

1. In the Admin Portal, click **Settings**, then click **Enrollment** to display available settings.
2. Click **Enrollment Codes**.
3. Click **Add**.
4. Select the details to be used to generate the enrollment code.

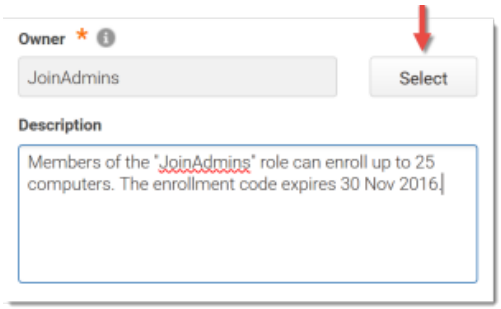
- Set an expiration date if the code should expire.



- Specify the maximum number of computers that can be enrolled if there should be a limit.



- For the Owner, click **Select** to select a role to control who will own the computers being added.
- (Optional) Enter a description for the enrollment code.



If you click **Save**, an enrollment code is generated without any IP address restrictions or System Set configuration. If you want to limitenrollment to computers matching certain IP patterns, you should click IP Range Restriction before clicking Save.

5. Click **IP Range Restrictions** to specify the IP addresses where the code is valid.

   Only computers with a client installed and an IP address within the ranges specified can be added to the Privileged Access Service using the enrollment code.

6. Click **Import Corporate IP Range** to automatically add your existing network IP range or click **Add** to specify IP ranges manually.

   You can also add addresses after importing your corporate IP addresses. For example, you might want to add IP addresses that are outside of the corporate firewall.

7. Click **System Sets Allowed** to associate a group of systems with attributes in common (system set) to an enrollment code.
   - Select the check box to allow system sets to be associated with an enrollment code.
   - Select **No Restrictions** to allow any system set to be enrolled using an enrollment code or select **Specified System Sets only** to select which system sets are allowed for enrollment using an enrollment code. If you select to only allow Specified system sets, you need to select the system sets that are allowed from the drop down menu or add them to list.
8. Click **Role Membership** to specify which roles the system service account will be assigned to after enrollment.

   Preassigning roles to enrollment codes is particularly useful when using delegated machine credentials; preassigned roles allow you to automatically configure the machine accounts with the appropriate permissions.
   - Click **Add** to open the Select Role dialog box.
   - Select the desired role(s) and click **Add** to return to the Role Membership information.
9. Click **Save** to generate the enrollment code, then click **Copy** to copy it to the clipboard.
10. Download the Delinea Client package, if necessary.
11. Create a script that installs the Delinea Client software package, registers the computer, and enables secure shell (ssh) connections.

    For example, you might create a simple script similar to this:

```
#!/bin/bash
rpm -iv ftp://ftp.centrify.com/CentrifyCC-1.0.0-121.x86_64.rpm
sudo /usr/share/centrifycc/bin/cenroll --tenant aak0298.centrify.com \
--code A12B3CD-EF45-6789-G01H-123456789012 \
--features aapm,agentauth,dmc \
--agentauth Authorized
sed -i '/^PasswordAuthentication no/d' /etc/ssh/sshd_config
/etc/init.d/sshd restart

```

    In this example, the enrollment code (specified by the --code parameter in the above example) includes the rules for expiration, maximum number ofservers allowed to register, the role that owns the registered server, and the IP restrictions you have defined.

For more information about the Delinea Client and enrollment, see the following topics:

- "Enrolling and Managing Computers Using the Cloud Client for Linux" on page 53
- "Enrolling and Managing Computers with Cloud Clients" on page 41

Setting Profile Attributes for Clients

The Delinea Client for Linux is a software package you can install on Linux computers to support password management and authentication services for Privileged Access Service users. To support these features, the client

has a **service user** account. The service user requires some additional settings to have a valid profile on the Linux computer where services run or where you are authorizing client-based authentication for access.

To Set Profile Attributes for the Client Service User

1. In the Admin Portal > **Settings >Enrollment** to display the settings available for Privileged Access Service.
2. Click **Linux Settings**.
3. Select a default shell from the list of available shells to use for the client service user.
4. Specify the template to use for the home directory for the client service user.
5. Click **Save**.

Setting Group Visibility for Clients

If you use Privileged Access Service to support authentication services, you can select the Privileged Access Service roles you want to make available as valid groups on registered computers.

> **Note:** You can only view or delete roles from the Group Visibility page; you cannot add new roles to this page. Instead, you can make any role in Privileged Access Service available as a local group by editing the role directly.

To Make a Role Visible as a Valid Group for Clients

1. In the Admin Portal, click **Settings >Enrollment** to display the settings available for Privileged Access Service.
2. Click **Group Visibility** under the Delinea Agent section.
3. Click **Add**.
4. Type a search string or scroll to locate a role you want to make visible as a group on registered computers, then click **Select**.

> **Note:** Role names that are available as valid groups on registered Linux computers and include one or more commas (such as role,name) aredisplayed on Linux computers as a concatenation of the role name, wherecommas are replaced with underscores and a random suffix is appended to theend of the name (for example, role_name_FNVO). Subsequent queries on the name (role,name or role_name_ FNVO) return the same result (role_name_FNVO).

Selecting User Preferences

By default, secure shell and remote desktop sessions open a web-based browser client to connect to target systems when you select the Login action. You can set a user preference to specify the default window size for these remote sessions to adjust to different display requirements. You can also set user preferences to specify a local client application as an alternative to the default web-based browser client. If you prefer to use a local Mac or Windows-based client for remote connections, you can select the client to use. You then have the option to

download the Remote Access Kit that includes a client launcher application to your local Mac or Windows computer.

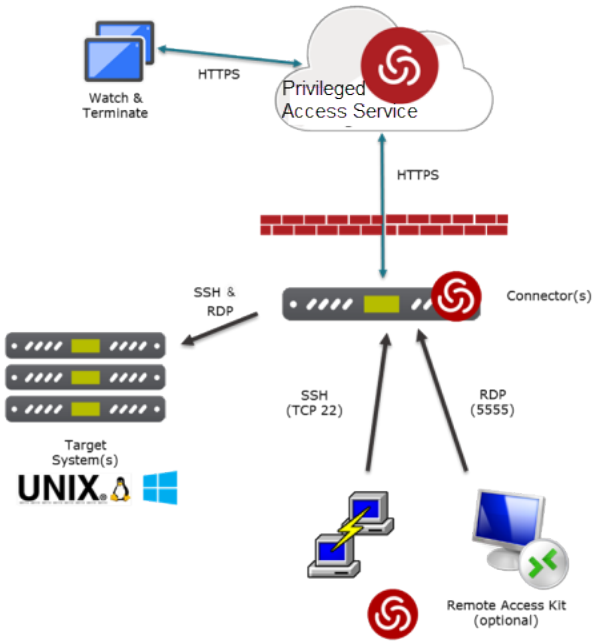
The Remote Access Kit client launcher enables you to start sessions using the selected client with a downloaded RDP configuration file instead of copying and pasting a command. If you download the client launcher and trust the website detected for the current cloud server, Privileged Access Service

adds the host name to a list of trusted websites for launching the local Mac or Windows-based client. You can add other host names to the list of trusted websites or remove host names from the list to ensure the arguments used to invoke the local client are only passed from the secure websites that you trust. For more information about using the Remote Access Kit client launcher and a local Mac or Windows-based client to connect to target systems, see "Using Local Windows-based Clients" on page 713.

> **Note:** Downloading the Remote Access Kit is optional. The Remote Access Kit client launcher only applies if you are running a client–such as PuTTY or remote Desktop Session Host (mstsc)–on a local Windows computer. You must use the client launcher to maintain the list of host name URLs for trusted websites in the registry on the computer that hosts the local Windows-based client. Using the Remote Access Kit client launcher also ensures that activity is recorded in a log file.

The computer you use to log in to Privileged Access Service must be inside the corporate network or connected to a trusted website to use the local Mac and Windows-based client.

The following diagram illustrates an overview of using a local Windows-based client for remote sessions.



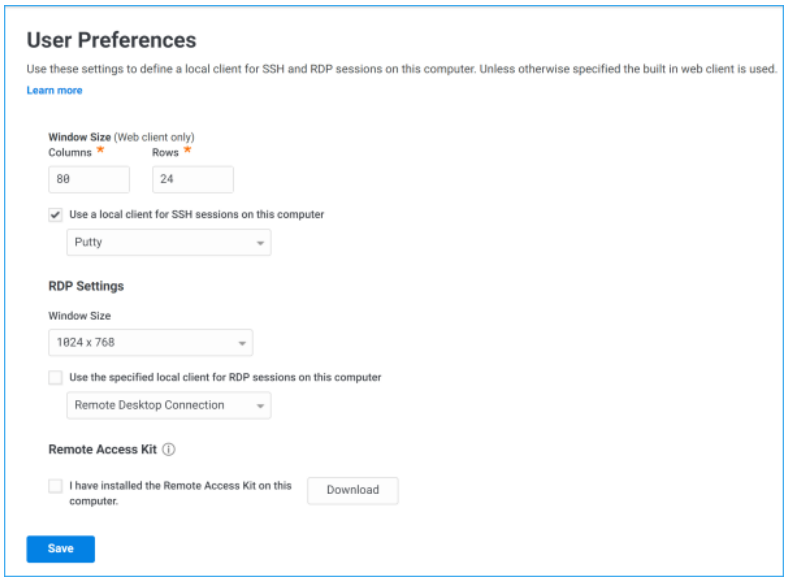
For more information about ports and protocols used between components, see "Review the Firewall Rules" on page 6.

To Set User Preferences for Remote Connections

1. In the Admin Portal > **Settings > Resources** to display the settings available for the Privileged Access Service.
2. Click **User Preferences**.
3. Set **Columns** and **Rows** to change the size of the window for secure shell sessions when using the web-based browser client.
4. If you want to use a local client for SSH sessions, select **Use a local client for SSH sessions on this computer**, then select a client such as **PuTTY**.

   Note: The PuTTY client must be available in the PATH folder for the service to invoke the PuTTY client.

5. Select a **Window Size** setting to change the size of the window for remote desktop sessions.
6. If you want to use a local client for RDP sessions, select **Use the specified local client for RDP sessions on this computer**, then select a client such as **Remote Desktop Connection**.



   Note: The use of web client may be disabled by the administrator. If administrator disabled, the option is grayed out.

7. (Optional) Click **Download** to download the Remote Access Kit, then open the downloaded file and follow the prompts displayed.
   - If you trust the website for the current cloud server, click **Yes**.
   - When the installation completes, select **I have installed the Remote Access Kit on this computer**, then click **Test**.

     If you do not install the Remote Access Kit and you do not select the check box saying that you did, you will see a dialog box telling you how to launch the native client yourself.
   - For SSH, the dialog box displays the command line for launching PuTTY.

For RDP, the dialog box prompts you to download the RDP file you want to use to launch a Windows Remote Desktop Connection.

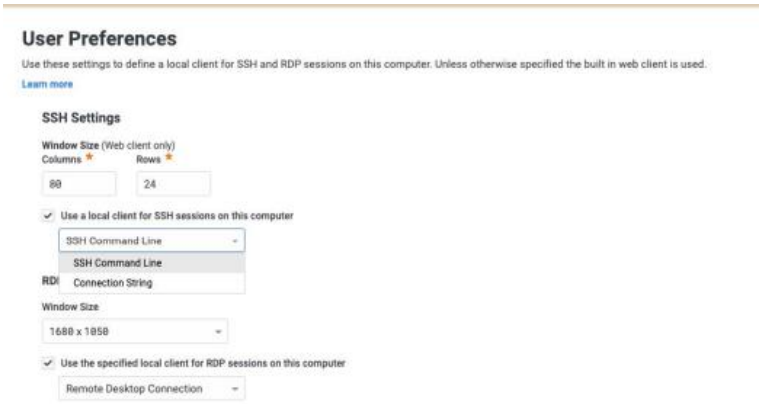
8. Click **Save**.

To use a native secure shell client without any interaction with the Admin Portal, see "Accessing Remote Systems" on page 701.

Mac-specific User Preferences

The following user preference option is available on Mac machines distinct from Windows as follows:

- There are two SSH options for the "Use a local client for SSH sessions on this computer" option in Mac:
  - SSH Command Line: This option works with the built-in terminal application in Mac by allowing you to copy the command and paste it into terminal.
  - Connection String: This option works with SSH applications such as Putty for Mac.



Viewing or Deleting Configuration Files

You can view the configuration files that you have previously deployed to your enrolled Linux systems in the the Settings > Resources > Config Files area.

You can also delete any or all of these configuration files. Be aware, though, that deleting the configuration files from the Admin Portal does not remove them from systems where you have deployed them.

For details on deploying configuration files, see "Deploying the user.ignore and group.ignore Configuration Files" on page 688.

To delete configuration files from the Admin Portal

1. Go to **Settings** > **Resources** > **Config Files**. The Config Files page displays all configuration files that you have deployed to Linux systems.

2. Select one or more files, and then click **Action** > **Delete**. The service removes the configuration files from the Admin Portal.

Installing and Configuring SafeNet KeySecure

If you want to store account passwords in SafeNet KeySecure, you must first install the appliance by following the instructions in the *KeySecure Installation and Configuration Guide*. As part of the initialization process, you will have created an admin account and specified the IP address, subnet mask, default gateway, host name, and port number for connecting to KeySecure. You should take note of the IP address or fully-qualified domain name and port number used for the appliance.

You can use the following SafeNet KeySecure models to provide centralized key management and store passwords for the Privileged Access Service:

- SafeNet KeySecure K460
- SafeNet KeySecure K450
- SafeNet KeySecure K250
- Virtual KeySecure Key Management

Interoperability between the Privileged Access Service and the KeySecure appliance requires the Key Management Interoperability Protocol (KMIP), version 1.1, the KeySecure appliance operating system version 8.1 or 8.2, and ProtectApp version 8.1. Note that these are the basic integration requirements. You should check the release notes for any additional or updated requirements before proceeding.

Note that you must have the SafeNet KeySecure appliance installed and configured in your environment and available on the network before configuring it for storage of Privileged Access Service passwords.

After the initialization process is complete, you must configure KeySecure with at least one server certificate for communication between KeySecure and the Delinea Connector. To generate a valid server certificate, you must have a certificate authority (CA) sign the certificate request. You can create a local CA certificate for KeySecure using its management console, then use the local CA certificate to sign the certificate requests. If you don’t create a local certificate authority, you must use an external certificate authority to sign certificate requests.

To prepare for password storage in KeySecure, you need to do the following:

- "Create or Identify the Certificate Authority (CA) Certificate" on page 770
- "Create or Identify a KeySecure Server Certificate" on page 771
- "Create a Key Server Instance" on page 772
- "Select the client certificate to use for the connector" on page 773

Consult with your SafeNet KeySecure administrator or security officer to create or identify the KeySecure server certificate and client certificate to use with the connector. You can use any standard PKCS 12-compliant package, such as makecert or openssl, to create the certificates to use with the connector. Alternatively, you can use the Delinea-issued client certificate for the connector. If you use the Delinea-issued client certificate, you must download and import the Delinea CA certificate to enable two-way authentication between the KeySecure appliance and the Delinea Connector.

The following figure provides an overview of the certificates required.

For complete information about installing and configuring a SafeNet KeySecure hardware security appliance, see the *KeySecure Installation and Configuration Guide*.

Protecting Stored Passwords

If you store account passwords for the Privileged Access Service on a SafeNet KeySecure appliance, you should plan for appliance maintenance and periodically back up the appliance to protect all of the passwords you have stored there. For information about how to backup a KeySecure appliance, see the *SafeNet KeySecure User Guide*.

Migrating Passwords from one Location to Another

If you change the password storage location, the location does not change for any existing passwords. For example, if you have existing passwords stored in the Privileged Access Service, then change the storage location to SafeNet KeySecure, the existing passwords remain in the Privileged Access Service and all new passwords are stored in KeySecure. To move passwords to the new password storage location, you must create a password migration job which runs in the background. You can migrate passwords immediately after changing the storage location or at any later time, if needed.

To move existing passwords to a new storage location:

1. Open the administrative portal from the account name menu.
2. Click **Settings > Resources**.
3. Select **Password Storage** from the list of settings.
4. Click **Migrate Passwords** to create a password migration job.

Specify the email address where you want to receive notification of the migration results, then click **Yes**.

After you start the job, you can view the status and results of the job by clicking **View Migration Job Status and Reports** or wait to receive email notification that migration is complete. The email notification will provide a link to the job history. You can then click the link in the email to see details about the migration results. Because job history reports can list details for different types of jobs, you can use the Search field to filter the jobs displayed.

Working with Appliances in a Cluster

You can configure SafeNet KeySecure appliances and clients to use multiple tiers to support high availability, disaster recovery, and load balancing. All of the appliances configured as a cluster in the same tier automatically perform load balancing within that tier. The Centrify Connectors that you install and configure for communication with KeySecure appliances will automatically try to connect to the appliances in the first tier in a “round robin”

sequence. If all of the appliances in the first tier go down, however, the connectors will attempt to connect to the appliances in the second tier.

To configure communication for multiple appliances in multiple tiers, you can use the following formatting convention for the KeySecure IP addresses:

- Use a colon (:) to separate the IP addresses within the same tier.
- Use a pipe character (|) to separate the IP addresses in different tiers.

For more information about configuring communication for multiple appliances in multiple tiers, see the following topics:

- "Configuring Clustering for Load Balancing or Failover" on page 773
- "Configuring Clustering for Load Balancing and Failover" on page 774

Deleting a SafeNet KeySecure Configuration

If you want to change your password storage location–for example, to use a different hardware appliance or to store passwords in the Privileged Access Service–you might want to delete an existing KeySecure configuration. You should note that you can only delete an existing SafeNet KeySecure configuration when there are no passwords stored in the appliance. Before attempting to delete the configuration, migrate all of the passwords you have stored in the appliance to the Privileged Access Service. For more information about password migration, see "Migrating Passwords from one Location to Another" on the previous page.

To delete the SafeNet KeySecure configuration:

1. In the Admin Portal, click the **Settings** tab.
2. Select **Resources> SafeNet KeySecure Configuration** and scroll to the bottom of the page.
3. Click **Delete Configuration**.
4. Click **Yes** to confirm that you want to delete the configuration settings.

[title]: # (Create or identify the certificate authority (CA) certificate) [tags]: # (config file,delete,configuration file) [priority]: # (121)

Create or Identify the Certificate Authority (CA) Certificate

Depending on the requirements of your organization and the configuration of your KeySecure appliance, you might have different options for creating or identifying the CA certificate to use for authentication. For example, one simple approach would be to create a local certificate authority for the KeySecure appliance as a self-signed root certificate. Alternatively, you might create a local CA certificate through an intermediate CA request or select an existing CA certificate that you use for other services.

Regardless of the method you use to create or identify the KeySecure CA certificate, you will need to upload the CA certificate to the Privileged Access Service. The steps in this section describe how to create a local certificate authority as a self-signed root certificate.

To create a new local certificate authority:

1. Log on to the KeySecure management console as an administrator with permission to access Certificate Authorities.
2. Click the **Security** tab to display the Device CAs and SSL Certificates section, then click **Local CA**.
3. Under Create Local Certificate Authority on the Certificate and CA Configuration page, enter the appropriate information for all fields.
4. Select either **Self-signed Root CA** or **Intermediate CA Request** as the certificate authority type.

If you create a self-signed root CA, you must also specify certificate duration and a maximum user certificate duration. If you are creating a self-signed root CA, you must also manually add it to the list of trusted CAs before it can be used.

If you create an intermediate CA request, you must sign the request using an existing trusted intermediate CA or your organization's root CA. When creating an intermediate CA request, you must also specify a maximum user certificate duration when installing the certificate response. The user certificate duration cannot be longer than the signing CA certificate's duration.

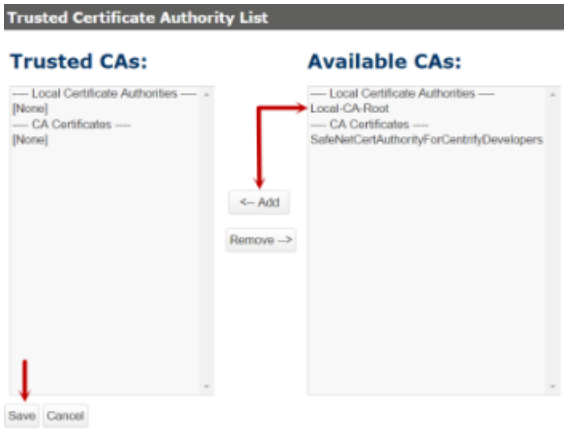
5. Click **Create** to create the local certificate authority for KeySecure.

If the local certificate authority is a self-signed root certificate, there are a few additional steps.

6. Under Device CAs and SSL Certificates, click **Trusted CA Lists**.
7. Under Trusted Certificate Authority List Profiles, select Default or another profile, then click **Properties**.

Alternatively, you can click Add to create a new profile, then select the new profile and click **Properties**.

8. Click **Edit** to add the local CA certificate to the list of trusted CA certificates.
9. Select the self-signed root CA from the list of Available CAs, click **Add**, then click **Save**.



Create or Identify a KeySecure Server Certificate

After you have created a local certificate authority with its corresponding CA certificate, you can use that certificate to sign the KeySecure server certificate. You can use the KeySecure management console or another tool to create the server certificate, but you must have an active CA-signed server certificate to establish SSL connections with client services. To create the server certificate, you must create a certificate request and sign the request with the

local CA. The steps in this section describe how to create a server certificate signed by the local certificate authority using the KeySecure management console.

To create a server certificate:

1. On the Security tab, under Device CAs and **SSL Certificates**, click SSL Certificates.
2. Under Create Certificate Request on the Certificate and CA Configuration page, enter the appropriate information for all fields.
3. Click **Create Certificate Request**.

The request appears in the certificate list with a status of Request Pending.

4. Select the request, then click **Properties**.
5. Copy all of the certificate request text starting with -----BEGIN CERTIFICATE REQUEST----- through the -----END CERTIFICATE REQUEST----- string.

Do not copy any extra white space.

6. Under Device CAs and SSL Certificates, click **Local CA**.
7. In the Local Certificate Authority List, select the local CA, then click **Sign Request**.
8. Paste the certificate request into the Certificate Request field.
9. Select **Server** as the certificate purpose, specify a certificate duration, then click **Sign Request**.

The newly-activated certificate displays on a new page.

10. Copy the certificate text starting with -----BEGIN CERTIFICATE----- through the -----END CERTIFICATE----- string.
11. Under Device CAs and SSL Certificates, click **SSL Certificates**.
12. Select the server certificate request, then click **Properties**.
13. Click **Install Certificate**.
14. Paste the text from the signed certificate into the Certificate Response field, then click **Save**.

When you return to the main Certificate and CA Configuration page, the server certificate is now an active certificate. It can be used in to establish SSL connections with client services.

Create a Key Server Instance

The next step is to create a dedicated key server instance for the exchange of keys between the KeySecure appliance and the connector client. Adding a new key server instance specifically for communication between the KeySecure server and the Centrify Connector is not strictly required. However, this is the recommended approach to isolate the communication channel.

To create a new key server instance:

1. Click the **Devices** tab to display the Cryptographic Key Server Configuration.
2. Click **Add** to create a new key management server instance.

The options to add, edit, and delete key server instances are restricted. If you don't see these options, you need to log on using different administrative account credentials.

3. Select **KMIP** as the server protocol, type the port number and select **Use SSL**, then select the KeySecure server certificate from the list of available certificates.
4. Click **Save**.
5. Click the **Security** tab, then under Device CAs and SSL Certificates, click **Local CA**.
6. Select the local CA certificate, then click **Download**.

The certificate you download in this step is the certificate you need to upload to the Privileged Access Service to enable secure communication between the KeySecure appliance and the connector.

7. Rename the downloaded file to use the **.cer** file extension.

Select the client certificate to use for the connector

To ensure secure communication between KeySecure and the Centrify Connector, you need to have a signed client certificate. Depending on your environment and tools available, you might select one of the following options:

- You can create a new client certificate using the KeySecure management console or another tool to use for the Centrify Connector. This option is similar to creating the server certificate except that you select Client for the Certificate Purpose.
- You can use an existing client certificate that you use for other secure services.
- You can use the certificate created by the Privileged Access Service.

The first two options assume you are signing the certificate with a trusted local certificate authority and require you to upload the signed client certificate to the connector. The third option requires you to download the Centrify CA certificate onto the KeySecure appliance. After you have selected an option for obtaining the client certificate, you have all of the information required to configure SafeNet KeySecure as the password storage location for the accounts you add to the Privileged Access Service.

For complete information about installing and configuring a SafeNet KeySecure hardware security appliance, see the *KeySecure Installation and Configuration Guide*.

Configuring Clustering for Load Balancing or Failover

Note that you can use the special separator characters together or independently to suit different configuration scenarios. For example, you can use the colon between IP addresses to distribute network traffic more or less equally for load balancing in a site. If you use the pipe character between IP addresses, the first IP address listed is the master with password changes replicated on the appliance specified by the second IP address. In this scenario, password changes would only be sent directly to the second IP address if the appliance in the first tier is not available.

In both cases, clustering support is implemented using the SafeNet KeySecure client libraries through the Centrify Connector.

Configuring Clustering for Load Balancing and Failover

Depending on your network topology, you might want to use the special separator characters together to suit more complex configuration scenarios. For example, you might configure the maximum of three tiers for your cluster, but support load balancing within each tier. To illustrate this scenario, you might have appliances with the following IP addresses:

- First tier: 192.168.1.2:192.168.1.3
- Second tier: 192.168.1.4:192.168.1.5
- Third tier: 192.168.1.6:192.168.1.7

When configuring communication for these tiers, you would specify the addresses and tiers like this:

192.168.1.2:192.168.1.3|192.168.1.4:192.168.1.5|192.168.1.6:192.168.1.7

This example would be translated to the following key server instances:

KMIP_IP.1=192.168.1.2:192.168.1.3 KMIP_IP.2=192.168.1.4:192.168.1.5 KMIP_IP.3=192.168.1.6:192.168.1.7

The connectors will always try to connect to the appliances in the first tier, distributing the workload to both the 192.168.1.2 and 192.168.1.3 appliances. If the appliance with the IP address 192.168.1.2 goes down, all connector traffic is routed to the appliance with the IP address 192.168.1.3. The connector will continue to use only the appliances in the first tier as long as there are appliances available in that tier. If no appliances are available in the first tier—that is, both 192.168.1.2 and 192.168.1.3 become unavailable—the connector will try to connect to the appliances in the second tier.

In most cases, the appliances in different tiers are configured in separate sites, so that appliances in the first tier are closest in the network topology to the client computer—in this case, the connectors—to ensure the best performance. Appliances in the second and third tiers might be in remote sites where the performance is poorer but are only used as a matter of last resort if no appliances in the primary tier are available.

Because clustering support is implemented using the SafeNet KeySecure client libraries, you should refer to your KeySecure documentation for additional information about configuring an appliance cluster.

Request and Approval Workflow Overview

While it is possible to give users access by statically assigning them to a role with specific administrative rights, a more secure method for controlling access is to establish a request and approval workflow. A request and approval workflow gives specific users or members of specific roles the ability to approve or reject access requests. A request and approval workflow improves security by controlling which users can request access, which users can grant access, and how long access is allowed if it is granted.

If you are a member of the System Administrator role or have the appropriate permissions, you can configure a request and approval workflow for different types of access requests. The procedure for configuring the workflow depends of the type of access request and the service offerings you use.

Note: If **Workflow** is enabled on the user's account, and the user requests permission using **Request Checkout**, the password can only be checked out during the time period specified by the admin. For example between 1pm - 2pm. This adjusts the checkout duration to ensure the password is checked back in by the end of the time period. For example 2pm.

We provide a number of ways of configuring workflow, depending on the kind of situation. Some require a connector to be installed on the system, some require the system to be enrolled in the service with the Cloud Client, and some require that the Server Suite Agent is installed on the system.

Workflow Type	Use Case Description	Requires a Connector?	Requires a Server Suite Agent?	Is there a global setting?	
Zone role workflow	A user wants permissions to do something on a Linux or Windows system	Yes	No	Yes	
Zone role workflow	A user wants permissions to do something on a Linux or Windows system	Yes	No	Yes	
Privileged account workflow	A user wants permissions to use a vaulted account	Yes	No	No	Yes
Application workflow	A user wants permissions to access an application	Yes	No	No	
Client-based worfklow / Agent Auth workflow	A user wants permissions to log in to a Linux or Windows system using the Cloud Client	No	Yes	No	
Privilege elevation workflow	A user wants permissions to run privileged commands on an enrolled system	No	Yes	No	

For details about configuring a request and approval workflow for a specific type of access request, see the following topics:

- "Using Zone Role Workflow" on the next page for details about allowing Active Directory users who are registered as Privileged Access Service users to request a role assignment on a computer that is joined to a Server Suite zone.
- "Using Privileged Account Workflow" on page 785 for details about managing account password checkout access requests and login access for systems, domains, and databases if you have Server Suite deployed.
- "Managing Application Access Requests" on page 794 for details about managing application access requests to specific applications if you have Application Services deployed.

- "Using Agent Auth Workflow" on page 801 for details on how to enable global login workflow for privileged accounts.
- "Privilege Elevation Workflow" on page 102 for details about how to enable and use privilege elevation workflow.

If you are managing Privileged Access Service on your internal network or a private cloud, you can configure a request and approval workflow. However, request and approval messages require you to have a mail server for outgoing email requests. You can configure the settings for a custom Simple Mail Transport Protocol (SMTP) mail server in the administrative portal. For details about post-installation configuration steps when you deploy Privileged Access Service as a self-managed service, see the *Installation and Configuration Guide for On-Site Deployment*.

Using Zone Role Workflow

Zone role workflow allows you to set up a workflow process so that access to computers in Server Suite zones can be requested, approved or rejected, and tracked.

With zone role workflow:

1. Users can request assignment to a role that's defined for a specific computer in a Server Suite zone.
2. After the user requests the zone role assignment, the approver can grant access either temporarily or permanently or reject the request to deny access.
3. Once the approver grants access by approving the request, the service assigns the user to the zone role on that computer and updates Active Directory automatically. The user now has all the privileges defined in that zone role.

When you enable your deployment to use zone role workflow, you also specify the following:

- Which users can submit requests
- Which users can approve requests
- Which systems can have access requested and approved
- Which zone roles a user can request that are available on the specified systems

You can enable and configure zone role workflow at the domain level. After you enable and configure a workflow at the domain level, all systems in the domain use that zone role workflow by default. You can then override or disable the default workflow at the system level. The system-specific settings that you specify override the domain settings.

For example, you might enable and configure zone role workflow at the domain level to establish default settings for role availability, approvers, and requestors. Then, you can use system-specific settings to have individual systems opt out of the zone role workflow or to override role availability and approver settings for specific systems.

Users requesting zone role assignment must be domain users, and must be assigned at least one administrative right with access to the Privileged Access Service with permission to View objects in the Admin Portal.

Approvers do not need to be domain users. Approvers can be specified individually, or by group membership.

Zone Role Workflow Setup Overview

Here's an overview of how you set up your deployment to use zone role workflow.

How to set up zone role workflow (an overview):

1. Make sure your deployment meets the prerequisites.

   For details, see "Zone Role Workflow Requirements" below.

2. (Optional but recommended) Create roles for requestors and approvers.

   For details, see "Creating Roles for Requesters and Approvers" on the next page.

3. Enable a default zone role workflow for the domain. Here you'll also assign the roles that you created in the previous step.

   For details, see "Enabling Zone Role Workflow" on page 779.

4. Configure which users can request zone-based role assignments.

   For details, see "Configuring Users to Be Requestors" on page 781.

5. Configure who can approve zone role workflow requests.

   For details, see "Configuring Users and Roles to be Approvers" on page 782.

6. (Optional) Customize the email that is sent and for which kinds of zone role workflow actions.

   For details, see "Customizing the Notification Email for Zone Role Workflow Activity" on page 783.

Zone Role Workflow Requirements

In order to configure your deployment for zone role workflow, ensure that your deployment meets the following requirements:

- "Infrastructure Requirements" below
- "Join Requirements" below
- "Domain Requirements" on the next page

Infrastructure Requirements

Privileged Access Service for identity and privilege elevation must be installed and running on at least one computer in the domain, and the Privileged Access Service must be configured with at least one zone.

The computers you add to the Privileged Access Service for zone role workflow must be added using the fully-qualified DNS name, not the IP address, and must be serviced by a Cloud Connector, have a domain specified, and be enabled for domain operations. Computers that are discovered automatically will automatically be associated with a connector, have their domain set, and be enabled for domain operations.

If you add a computer manually, you must also manually specify a domain and enable domain operations for that computer. For details about specifying domains for systems and enabling domain operations, see Setting domain operations for a system.

Join Requirements

Computers participating in a zone role workflow must be joined to a zone.

- Linux and UNIX computers must have the Server Suite agent installed, and be joined to an Active Directory domain and a zone with the adjoin command.
- Windows computers must be joined to an Active Directory domain, have the Server Suite Agent installed, and the agent must be joined to a Server Suite zone.

To see whether a computer is joined to a zone:

1. Open the Admin Portal, click **Resources**, then click **Systems**.
2. Select a system to view its details, then click **Advanced**.
3. Check the Zone Joined Status field to verify it displays “Joined.”

   If necessary, you can manually update the joined status for a computer. For more information about using the Advanced tab, see Setting system-specific advanced options.

The Privileged Access Service periodically updates the zone joined status of systems in the domain. Use the **Domains > Advanced** tab as described in Setting domain-specific advanced options to view and change the update interval.

Domain Requirements

You must have a domain administrative account with read and write permission in Active Directory for each domain that participates in a zone role workflow. For details about creating domain administrative accounts, see Setting domain administrative accounts. If you select an Active Directory account as the domain administrative account, the account must be given permission in Server Suite to create assignments for the computers in participating zones.

In addition, only domains that are discovered automatically by a Cloud Connector can be used in a zone role workflow by default because users requesting zone role assignments must be Active Directory users. If you add domains manually, you can manually assign the connectors to use for the domain.

To see whether a domain was discovered by a connector:

1. Open the Admin Portal, click **Resources**, then click **Domains** to view the list of domains.
2. Check the Discovered column to verify the domain has a value of “Auto” indicating that the domain was discovered automatically.

Creating Roles for Requesters and Approvers

This topic describes how to create one or more identity service roles for users who can request zone role assignment (requesters), and users or groups who can approve or reject zone role assignment requests (approvers).

This step is optional, but is typically done so that users and groups can easily be given request and approval permission by assigning them to the appropriate role.

To create roles for requesters and approvers:

1. Open the Admin Portal, click **Access**, then click **Roles**.
2. Click **Add Role**.
3. Provide a unique name for the role.

4. Click **Members**, then click **Add**.
5. Type a search string to search for and select users and groups for this role, then click **Add**.
6. Click **Administrative Rights**.
7. In the Add Rights dialog, select one or more of the following administrative rights so that the role has access to Privileged Access Service:
   - Privileged Access Service User
   - Privileged Access Service Power User
   - Privileged Access Service Administrator

   For more information about these rights, see Admin Portal administrative rights.
8. Click **Save** to save the role.

Enabling Zone Role Workflow

The Privileged Access Service will query Active Directory to find the roles available for assignment. When you select the roles you want to make available to requestors, you can see whether the roles are available for UNIX computers, Windows computers, or both. You can also modify whether the roles are available to UNIX, Windows, or both.

Enabling Zone Role Workflow for a Domain and Configuring the Available Roles

When you enable a domain for zone role workflow, you also specify which zone-based roles can be requested.

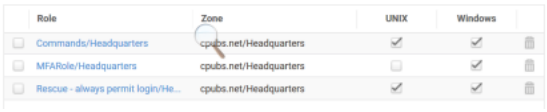
To enable a default zone role workflow for all computers in a domain:

1. Open the Admin Portal, click **Resources**, then click **Domains** to view the list of domains.
2. Select a domain to view its details.
3. Click **Zone Role Workflow**.
4. Select **Enable zone role requests for systems in this domain**.
5. Under Assignable Zone Roles, click **Add**.

6. Select a role you want to make available to requestors from the list of roles available for the domain, then click **Add**.

   To search for a role, start typing the name of the role. When you find the role you want to add, select it and click **Add**. You can add as many roles as you need by repeating Step 5 and Step 6.

7. Modify the role availability, if needed, then continue to .



Enabling Zone Role Workflow for a Specific Computer

To enable, configure, or override the workflow for a specific computer

1. Open the Admin Portal, click **Resources**, then click **Systems** to view the list of systems.
2. Select a system to view its details.
3. Click **Zone Role Workflow**.
4. Check **Use Domain Administrator Account for Zone Role Workflow operations** to enable zone role workflow for the system.

   When setting up zone role workflows, you can only request zone roles for a system whose zone status is joined. The status of a system is periodically refreshed but you can also select **Check Now** for an on-demand refresh of the zone joined status (also see Setting domain-specific advanced options). The zone joined status can be one of the following:

   - Joined–System is joined to a hierarchical zone.
   - Not Joined–System is not joined to any hierarchical zone.
   - Undetermined–he zone status was added using an IP address instead of a DNS (DNS is not specified).
5. In the **Enable zone role requests for this system** field, select one of the following choices:
   - Select **--** to use the default zone role workflow settings defined for the domain.
   - Select **Yes** to define zone role workflow settings specific to this computer. The settings that you define here override the domain settings. Note that only users with the **Edit** permission for the system and the system domain, can enable zone role workflow for the system (see Setting domain-specific permissions and Setting system-specific permissions).
   - Select **No** to disable zone role workflow for this computer even if it is enabled at the domain level.

     If you select **--** or **No**, click **Save** to save your changes.
6. If you selected **Yes**, under Assignable Zone Roles, select one of the following choices:
   - Select **Use domain assignments** to use the roles defined for the domain.
   - Select **Choose** to override the roles defined for the domain.
7. If you are overriding the roles defined for the domain, click **Add** to search for and select a role you want to make available to requestors from the list of roles available for the domain.
8. Select one or more roles, then click **Add**.

   You can add more roles by repeating Step 6 and Step 7.
9. Modify the role availability, if needed, then continue to "Configuring Users to Be Requestors" on the next page.

Configuring Users to Be Requestors

You must give requestors—whether they are individual users or members of a roles—the right to submit zone role requests. You can grant the permission to submit zone role requests on individual systems, on system sets, or globally for all systems.

Creating a system set is optional but simplifies zone role assignments. For information about creating system sets, see Adding system sets.

Assigning Requestors for Systems and Sets

The process of assigning who can request a zone-based role assignment involves adding the users to the system's permissions and making sure that the user accounts have the right permissions.

To assign users or groups as requestors for systems and system sets:

1. Open the Admin Portal, click **Resources**, then click **Systems** to view the list of systems.
2. Select an individual system or a system set.
   - If you are viewing the details for an individual system, click **Permissions**.
   - If you select a system set, right-click to select **Modify**, then click **Member Permissions**.
3. Click **Add** to search for and select the users, groups, and roles to which you want to grant permissions.

   To find a user, group, or role to add, start typing the user, group, or role name. When you find the user, group, or role you want to add, select it and click **Add**.
4. On the Permissions page for the system, select the **View** and **Request Zone Role** permissions for each user, group, and role allowed to submit zone role access requests.
5. Click **Save**.

   The users, groups, and roles that you specified now have permission to request zone-based role assignment on the individual system or system set that you selected.

Assigning Global Requestors

If desired, you can assign global system permissions to some users so that they have zone role workflow permissions on all systems by default.

To assign global zone role request permissions:

1. Open the Admin Portal, click **Access**, then click **Global System Permissions**.
2. Click **Add** to search for and select the users, groups, and roles to which you want to grant permissions.

   To find a user, group, or role to add, start typing the user, group, or role name. When you find the user, group, or role you want to add, select it and click **Add**.
3. Select the **View** and **Request Zone Role** permissions for each user, group, and role allowed to submit zone role access requests.
4. Click **Save**.

   The users and roles that you specified now have permission to request zone role assignment on all systems by default.

Configuring Users and Roles to be Approvers

To complete the zone role workflow, you need to specify which users, groups, and roles can approve or reject zone-based role assignment requests for all computers in a domain or for specific computers.

Configuring Approvers for the Domain

If desired, you can specify some users to be zone role workflow approvers for all systems in a domain.

To configure approvers for the domain:

1. Open the Admin Portal, click **Resources**, then click **Domains** to view the list of domains.
2. Select a domain to view its details.
3. Click **Zone Role Workflow**.
4. Under Approver List, click **Add**.
5. For the Approver Type, select either **Requestor's Manager** or **Specified User or Role**.
   - If you select **Requestor's Manager**, select the action to take if the requestor doesn't have a manager, then click **Add**.
   - If you select **Specified User or Role**, click **Add** to search for and select users, roles, or both.

     To find a user or role to add to the approver list, start typing the user or role name. When you find the user or role you want to add, select it and click **Add**. You can also select multiple approvers at once or repeat Step 4 and Step 5.
6. Click **Save** to save your changes to the approvers list, then continue to "Configuring users to be requestors".

Configuring Approvers for a Specific Computer

You can configure zone role workflow approvers for a specific computer, either as additional users or to override a domain-level approver setting.

To configure or override approvers for a specific computer:

1. Open the Admin Portal, click **Resources**, then click **Systems** to view the list of systems.
2. Select a system to view its details.
3. Click **Zone Role Workflow**.
4. Under Approver List, select one of the following choices:
   - Select **Use domain assignments** to use the approver users and roles defined for the domain.
   - Select **Choose** to override the approver users and roles defined for the domain.
5. If you are overriding the approver users and roles defined for the domain, Click **Add**.
6. For the Approver Type, select either **Requestor's Manager** or **Specified User or Role**.
   - If you select **Requestor's Manager**, select the action to take if the requestor doesn't have a manager, then click **Add**.
   - If you select **Specified User or Role**, click **Add** to search for and select users, roles, or both.

To find a user or role to add to the approver list, start typing the user or role name. When you find the user or role you want to add, select it and click **Add**. You can also select multiple approvers at once or repeat Step 5 and Step 6.

7. Click **Save** to save your changes to the approvers list.

Customizing the Notification Email for Zone Role Workflow Activity

You can use or customize the default email notification templates that the service sends out when there is any zone role assignment request activity.

To customize zone role assignment notification email:

1. Open the Admin Portal, click **Setting**, then **General**, then click **Account Customization**.
2. Scroll to locate the **Message Customization** section.
3. Select any of the following message templates to customize the content for zone role access requests:
   - Zone Role Assignment Request
   - Zone Role Assignment Approved
   - Zone Role Assignment Denied
   - Zone Role Assignment Request Failed

   For more information about customizing message templates, see How to customize email message contents.

Working with Zone Role Workflow

After you have configured your deployment for zone role workflow, you can use a workflow and its related features to request, view, and approve zone role assignment requests as described in the following topics:

- "Requesting Assignment to a Zone Role" below
- "Responding to Zone-based Role Assignment Requests" on the next page
- "Working with Zone Role Request Reports" on page 785
- "Confirming that Access is Denied After Expiration" on page 785
- "Viewing Zone Role Requests and History" on page 785

Requesting Assignment to a Zone Role

If you need access to a zone-based role assignment, you can submit a request to be assigned to that role assignment.

To request assignment to a zone role:

1. Open the Admin Portal, click **Resources**, then click **Systems** to view the list of systems.
2. Select the check box of a system to request access to a role for that system.
3. Click **Actions** and select **Request Zone Role** from the menu.
4. Select a role from the list and click **Request**.

5. Type a reason for your request, optionally provide ticket information, and optionally specify or modify the requested start and end time for the role assignment.
6. Click **Submit**.

   An email notification is sent to the user who will review and either approve or reject your request. You will receive email when the request is approved or rejected.

Depending on your environment, there could be a lag of up to an hour between the time you receive the email notification of approval and when your zone role assignment takes effect.

Responding to Zone-based Role Assignment Requests

If you are a user or member of a role that has been designated as an approver for zone-based role assignment requests, you can choose to approve or reject the zone-based role assignment requests that you receive.

Approving a Zone-based Role Assignment Request

If you are a zone role workflow approver, you will receive email notification whenever a request needing your approval is submitted. You can grant permanent access or temporary access that expires after a specified duration or time frame.

To approve a zone-based role assignment request:

1. Open an email message from Server Suite zone Role Assignment Management with the subject, “Zone role assignment request.”
2. Click the **View Request** link.

   If you are not already signed in to the Privileged Access Service, sign in when prompted.
3. Review the request details and click **Approve**.
4. Choose a duration or time frame for access:
   - To grant permanent access, select **Grant Permanent Permission**.
   - To grant temporary access for a specified duration, select **Grant Temporary Permission** and specify the number of minutes, hours, or days before expiration.
   - To grant temporary access for a specified time frame, select **Grant Windowed Permission** and specify a start time and an end time.

     The default values for windowed permission are provided by the requester in the original request. If multiple approvers are configured, only the first approver to respond can change those values.
5. Click **Submit**.

   The requester is notified of approval by email.

Rejecting a Zone-based Role Assignment Request

If you are a zone role workflow approver, you will receive email notification whenever a request needing your approval is submitted. If you do not approve of the request you can reject it.

To reject a zone-based role assignment:

1. Open an email message from Server Suite zone Role Assignment Management with the subject, “Zone role assignment request.”
2. Click the **View Request** link.

   If you are not already signed in to the Privileged Access Service, sign in when prompted.
3. Review the request details and click **Reject**. The Rejection dialog opens.
4. In the Rejection dialog, optionally provide a reason for the rejection.
5. Click **Submit**.

   The requester is notified of rejection by email.

Working with Zone Role Request Reports

A built-in report, “Zone Role Requests,” is provided to give you detailed information about zone-based role assignment requests. You can view, copy, email, and export a report for zone role assignment requests.

To access a zone role assignment request report:

1. Open the Admin Portal, click **Reports**, then click **Builtin Reports**.
2. Click **Zone Role Requests** to view to view the report or select the check box for **Zone Role Requests**, then click **Actions** to perform other actions, such as email or export the report.

   For more information about the actions that you can perform when working with reports, see Managing reports.

Confirming that Access is Denied After Expiration

After a zone-based role assignment expires, the role assignment is no longer valid on the computer where the role was assigned, and the requester can no longer use that role on that computer.

By default, expired zone-based role assignments are removed from Active Directory every six hours, so the expired role assignment might still be listed for up to six hours after it has expired, even though it cannot be used after expiration.

Use the **Resources > Domains > Advanced** page as described in Setting domain-specific advanced options to view and change the interval at which expired role assignments are removed from Active Directory.

Viewing Zone Role Requests and History

You can view the status and history of one or more zone-based role assignment requests.

To view request status and history:

1. Open the Admin Portal, click **Access**, then click **Requests** to view the list of requests.
2. Click on a request to view information about that request.

   The **Status** field shows whether the request is pending, approved, or rejected.

Using Privileged Account Workflow

As a member of the System Administrator role or a role with the Role Management administrative right, you can enable workflow for all other users. Initially, only the members of the System Administrator role have the ability to

enable a request and approval workflow. This also includes specifying the users or roles with authority to approve access requests. The workflow and approval authority can be configured to apply globally for all accounts or apply only for selected account and system combinations, or apply globally except where there are account-specific restrictions.

After you enable workflow for privileged account access requests, users can request access to the privileged local, domain, database, or service accounts that you specify. If the request is approved, the user can then check out the account password or use the account to log on to a system, domain, or database remotely.

Users requesting access must still be assigned to a role with Privileged Access Service Administrator or Privileged Access Service Power User administrative rights and have View permission to see the systems and accounts that are available in the Privileged Access Service. If a user is a member of a role with one of these rights, however, they can search or browse for systems and accounts, then submit a request to a designated approver for login access or for password checkout. The **approver** might be a specific user or any member of a specific role. If you configure a role as the approver, the first member to respond to the request is given the authority to approve or reject the request.

The steps involved in configuring a workflow include:

1. Create one or more roles that can **enable** a request and approval workflow.

   Members of the System Administrator role can enable workflow globally for all accounts. Users with the Privileged Access Service Administrator or Privileged Access Service Power User administrative right can enable workflow and select an approver for specific accounts where they have the Grant and Edit permissions.
2. Create one or more roles that can **approve** access requests for accounts.
3. Create one or more roles that can **request** access to privileged accounts.

   Any member of a role with the Privileged Access Service Administrator or Privileged Access Service Power User right can request access to any account where workflow is enabled. The appropriate permissions are granted if the request is approved.
4. Determine whether to enable the workflow globally for all accounts, individually for specific accounts, or a combination of both.
5. Enable the workflow option where appropriate and select the user or role with authority to approve requests.

The following topics describe how to configure request and approval workflow for account access requests, how to use a workflow to request account access, how to approve or reject a request, and how to view and manage requests that are being processed:

- "Enabling Workflow For Privileged Accounts" on the next page
- "Configuring Workflow Globally For All Accounts" on page 788
- "Requesting Password Checkout Access" on page 790
- "Requesting Login Access" on page 791
- "Responding to Access Requests" on page 792
- "Viewing Request Details" on page 793
- "Deleting Requests" on page 793
- "Customizing Account Workflow Notification Email" on page 794

Enabling Workflow For Privileged Accounts

The first few steps in configuring the request and approval workflow are optional and involve creating one or more roles for users who are allowed to define the request and approval workflow and the roles that can approve access requests. These steps are optional because you can choose to only allow members of the System Administrator role to be the users permitted to configure a workflow and members of the System Administrator role can assign approval authority to individual users without creating any approval roles. In most cases, however, creating roles for different sets of users provides greater flexibility and helps to reduce the number of requests left pending an approval.

Note: If you don't create any intermediary roles with the appropriate administrative rights to enable a workflow, only members of the System Administrator role will be able to configure any request and approval workflow you might want to implement.

If you are configuring a request and approval workflow for privileged accounts, you must create at least one role for users who are allowed to view systems and accounts. Only the members of a role with access to the Privileged Access Service and View permission can request login and password checkout access. Only members of the System Administrator role or a role with the Privileged Access Service Administrator or Privileged Access Service Power User administrative right can enable a request and approval workflow for stored accounts where they have the Grant and Edit permissions.

To configure roles that can enable a workflow:

1. Click **Access > Roles**.
2. Click **Add Role** or select an existing role to display the role details.
3. If you are creating a new role, you must provide at least a unique name for the role.
4. Click **Members**, then click **Add**.
5. Type a search string to search for and select users and groups for this role.
6. Click **Administrative Rights**, then click **Add**.
7. Select the appropriate rights, then click **Add**.
8. Click **Save** to save the role.

   For example, if you are creating a role with permission to enable a workflow for access to systems and accounts, select **Privilege Service Administrator** or **Privilege Service Power User**. You can select any additional rights you want included in this role, but you must select at least one of the required administrative rights.

   Only members of the System Administrator role can enable workflow globally for all accounts. Members of a role with the Privileged Access Service Administrator or Privileged Access Service Power User right can enable workflow for accounts where they have the Grant and Edit permissions.

Creating Roles For Approvers

You can assign approval authority to individual users. However, in most cases, creating "approver" roles for different sets of users provides greater flexibility and helps to reduce the number of requests left pending an approval. If you don't create any intermediary roles with the appropriate administrative rights to approve access requests, only members of the System Administrator role will be able to approve access requests. You can follow

the same steps described in "Enabling Workflow For Privileged Accounts" on the previous page to create roles for approvers.

Keep in mind that if you are creating a role with permission to approve access requests to stored accounts with managed or unmanaged passwords, you must include an appropriate administrative right with access to the Privileged Access Service in the role. You can select any additional rights you want included in this role, but you must select at least one of the required administrative rights.

Creating a Role with Access To Stored Accounts

In addition to the role that allows selected users to configure a workflow, you might want to create one or more roles for the users who will be requesting login and password checkout access to the systems and accounts stored in the Privileged Access Service. For those users to be able to search for or browse accounts and systems, they must be assigned to a role that includes the Privilege Service Administrator or Privileged Access Service Power User administrative right. You can follow the same steps described in "Enabling Workflow For Privileged Accounts" on the previous page to create the role. In most cases, you would add users who might need temporary administrative access as members of this role and give the role the Privileged Access Service Power User administrative right.

Configuring Workflow For Stored Accounts

As a member of the System Administrator role, you can configure a request and approval workflow globally for all accounts, for specific accounts, or using a combination of global and account and system-specific settings. As a member of a role with the Privileged Access Service Administrator or Privileged Access Service Power User administrative right, you can configure a request and approval workflow for specific accounts where you have Grant and Edit permissions.

For more information, see the following topics:

- "Configuring Workflow Globally For All Accounts" below
- "Configuring Workflow For Specific Accounts" on the next page

Configuring Workflow Globally For All Accounts

To simplify the process of configuring a request and approval workflow for privileged accounts, you can enable workflow as a feature that applies to all accounts stored in the Privileged Access Service. You can then select a single user or role to approve all login and password checkout requests. You can also use this global setting in conjunction with account-specific settings to selectively restrict access requests for some accounts or modify the user or role with approval authority. In other words, you can configure the approval workflow globally so that it applies for all resources and accounts, or on a per-resource and account basis, or using a combination of the two. If you use a combination of global-and account-specific approval settings, the account-specific approval settings take precedence over the global approval settings. For example, you might give members of the IT Outsource role global authority to approve login and password checkout requests for all resources and accounts, then identify specific system and account combinations where only members of the IT Supervisors role can approve access requests.

To configure workflow for all accounts:

1. Click **Settings > Resources > Global Account Workflow**.
2. Select **Enable Workflow for all accounts**.

3. Click **Select** and type a search string to search for and select a user or role with authority to approve login and password checkout requests, then click **Add**.
4. Click **Save**.

After you have configured the workflow for all accounts, users with Privileged Access Service Administrator or Privileged Access Service Power User rights can request login and password checkout access for the accounts stored in the Privileged Access Service.

Configuring Workflow For Specific Accounts

If you are a member of the System Administrator role or a member of a role with Privileged Access Service Administrator or Privileged Access Service Power User rights and have the Grant and Edit permissions, you can configure a request and approval workflow for specific accounts or use account-specific settings to override global workflow settings. If you enable or disable workflow for individual account and system combinations, the account-specific settings take precedence over the global settings. For example, you can use account-specific settings to prevent access requests for some accounts or to modify the user or role with approval authority.

To configure workflow for specific accounts:

1. Click **Resources > Accounts**, then select an account to display the account details.
2. Click **Workflow**.
3. Set the **Enable Account Workflow** to Yes if you want to select a user or role with authority to approve access requests.

   If you enabled workflow for all accounts, selecting Yes allows you to select a different user or role with approval authority. If you are not enabling workflow for all accounts, selecting Yes makes this specific account available for users requesting login or password checkout access.

   If you disabled workflow for all accounts, selecting No prevents users from requesting login or password checkout access.
4. Click **Save**.

After you have configured the workflow for an account, users can request login or checkout access to the account through the Privilege Manager portal.

Working with Privileged Account Workflow

Users who are assigned to a role with the appropriate administrative rights can see the systems, domains, databases, and accounts where they have View permission in the Privileged Access Service. What you can do depends on the additional permissions you have been granted. For example, if you don't have the Checkout permission, you cannot check out the password for a stored account. However, if one or more accounts are configured to use a *request and approval* workflow, you might be able to request access to the account password from a designated user or member of a designated role. It is at the approver's discretion to approve or reject your request, and if approved, to grant you permanent or temporary Checkout permission. For more information on available account permissions, see Additional account permissions.

If an account is configured to require the approval of a designated user or role, you might see the Request Login or Request Checkout actions in the **Accounts > Actions** menu. Selecting Request Login or Request Checkout sends an email request to the designated user or to the members of a designated role for approval. If your request is approved, you have limited period of time to take the action you requested.

In addition to requesting an account login or requesting to checkout a password, this section also includes information for the following:

- "Responding to Access Requests" on page 792
- "Viewing Request Details" on page 793
- "Deleting Requests" on page 793
- "Customizing Account Workflow Notification Email" on page 794

Requesting Password Checkout Access

If you are granted permission to checkout the password for a target system, you can access the system for the period specified. You can continue to use the session on the target system after the approved period of time expires as long as you don't exit the session. If you exit the session, however, and attempt to check out the password to start a new session after the temporarily approved period expires, you must submit a new Checkout access request.

Although you can check out local system account passwords on registered mobile devices, you cannot check out the password if the account has workflow enabled. If the password checkout for a local system account requires an approver, the Checkout feature on the mobile device is not supported.

To request a password checkout:

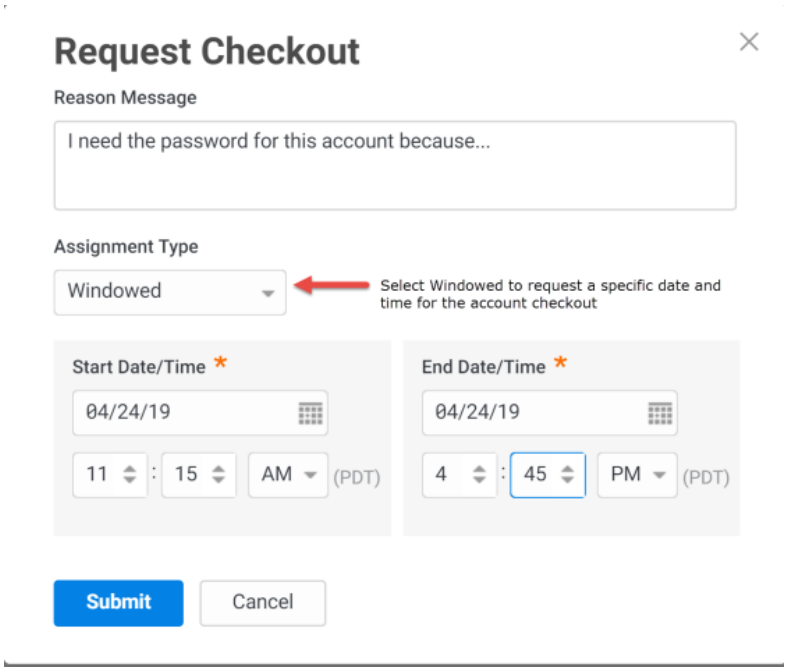
1. In the Admin Portal, click **Resources**, then click **Systems**, **Domains**, **Databases**, or **Accounts** to locate the account for which you want to check out a password.

   For example:

   - Click **Systems** if you want to check out the password for an account with access to a specific system name or system type.
   - Click **Domains** if you want to check out the password for an account with access to a specific domain.
   - Click **Databases** if you want to check out the password for an account with access to a specific database.
   - Click **Accounts** if you want to search or filter the accounts listed by account name or check the account health before requesting access to the password.
2. Select the account and open the Actions menu, then click **Request Checkout**.

   Note: If **Workflow** is enabled on the account, the password can only be checked out during the time period specified by the admin. For example between 1pm - 2pm. This adjusts the checkout duration to ensure the password is checked back in by the end of the time period. For example 2pm.
3. Type the business reason for requesting permission to check out the password.
4. Select whether you are requesting permanent access or access during a specific window of time.

   If you select **Windowed** access, specify the start date and time and the end data and time. For example:



5. Click **Submit**.

   An email notification of your request is sent directly to the designated approver and your request will be displayed on the Requests tab in the Admin Portal.

6. Click the **Requests** tab to see the status of your request.

   You will also receive an email notification when you request is approved or denied. If your request is approved and you have been granted temporary access, you will have a limited time to select the Checkout action. If the temporary approval period expires before you check out the password, you can submit a new request. Keep in mind that the request approval period is separate from the maximum password checkout time, which is controlled by a global- or object-specific policy.

Requesting Login Access

Users who are assigned to a role with the appropriate administrative rights can see the systems, domains, databases, and accounts where they have View permission in the Privileged Access Service.

What you can do when you select a system, domain, database, or account will depend on the additional permissions you have been granted. For example, if you don't have the Login permission granted, you cannot log on to target systems using stored account information. However, if one or more accounts are configured to use a "request and approval" workflow, you might be able to request access to a target system. Your request is sent to a designated user or member of a designated role for approval. It is at the approver's discretion to approve or reject your request, and if approved, to grant you permanent or temporary Login permission.

If your request is approved and you are only temporarily granted the Login permission, you will have a limited period of time in which to log on to the selected system using the selected account. If you are granted temporary Login permission, you can continue to use the session on the target system after the approved period of time expires. If you exit the session, however, and attempt to log on after the temporarily approved period expires, you must submit a new access request.

To request login access:

1. In the Admin Portal, click **Resources**, then click **Systems**, **Domains**, or **Accounts** to locate the account combination to which you want to request access.

   For example:

   - Click Systems if you want to search or filter the systems listed based on the system name or system type.
   - Click Domains if you want to search or filter the domains to which you want access.
   - Click Accounts if you want to search or filter the accounts listed by account name or check the account health before requesting access.

2. Select the account you want to use to log on to the target system or domain.

   Depending on how you navigate to the Actions menu, you can request access to an account in one of two ways:

   - If you open the Actions menu for a system, you can click **Select/Request Account** to search for and select the account you want to use.
   - If you open the Actions menu for a specific account, you can click **Request Login** to request access to that account.

3. Type the business reason for requesting permission to log on to the selected system using the stored account information.
4. Select whether you are requesting permanent access or access during a specific window of time.

   If you select **Windowed** access, specify the start date and time and the end data and time.

5. Click **Submit**.

   An email notification of your request is sent directly to the designated approver and your request will be displayed on the Requests tab in the Admin Portal.

6. Click the **Requests** tab to see the status of your request.

   You will also receive an email notification when you request is approved or denied. If your request is approved and you have been granted temporary access, you will have a limited time to select the system and account combination and the Login action. If you have been granted temporary access and the approval period expires before you log on, you can submit a new request.

Maintaining an Active Session After Approval

If your request is approved and you log on successfully before a temporary approval period expires, there's no time limit on your active session. However, an administrator with the appropriate permission can terminate the session.

In addition, you can log on multiple times during the approval period, if needed. For example, if you must restart a computer multiple times for maintenance—such as the installation or removal of software—you can do so until the request temporary approval period expires.

If you expect maintenance to require you to log on multiple times, you might want to request access for a specific window of time such as over a weekend or during a period when you know there will be little network activity.

Responding to Access Requests

There are no special privileges required to respond to requests. Anyone with access to the Privileged Access Service can be designated as an approver.

If you have been designated as an approver for login and password checkout requests, you will receive email notification when others request access. You can click the View Request link in the email to view the request details. If you are authorized to approve the request and the request is still pending a response, the Request Details displays the options to Approve or Reject the request.

- Click **Approve** to approve the request by granting permanent or temporary permission and specify a grant duration time in minutes, hours, or days. If you click Submit to continue with the approval, the request details are updated with the date and time the request was resolved and the approved status.
- Click **Reject** to reject the request and type the reason you are rejecting the request. If you click Submit to continue with the rejection, the request details are updated with the reason the request was rejected, the date and time the request was resolved, and the rejected status.

After you respond to the request, the Requests tab is also updated with the latest activity and email is sent to the requester as notification of your response to the request.

Viewing Request Details

If you have made or responded to a request, you can click the Requests tab to view the status of access requests and the history of request activity. You can click the Requests tab from the Admin Portal to see the status of your own pending requests, the requests awaiting your approval, or the results of request activity. You can then select any request displayed on the Request tab to see request details.

If you are an approver, you can also go directly to Request Details by clicking the link in the email notifying you of the request.

If you have the authority to approve requests and the request is still pending a response, you can click Approve or Reject from the Request details. For more information about approving or rejecting a request, see "Responding to Access Requests" on the previous page.

The request information table displays details appropriate for the current state of the request. For example, you might see the following information:

- Posted displays the date and time of the most recent activity for each request.
- Description provides a brief summary of the request indicating the type of access or application requested.
- Requestor displays the user who submitted the request.
- Requestor's Reason displays the business reason provided by the user who submitted the request.
- Approver displays the user or role designated for approving access requests if the approval is pending or the specific user who approved or rejected the request if the request has been resolved.
- Status displays the current status of the request as Pending, Approved, Rejected, or Failed.

  Depending on the status of the request, you might see the reason the request was rejected or the reason why the request failed.

Deleting Requests

If you have the Delete permission, you can remove requests from the Requests list if the request history is no longer needed.

To remove a request:

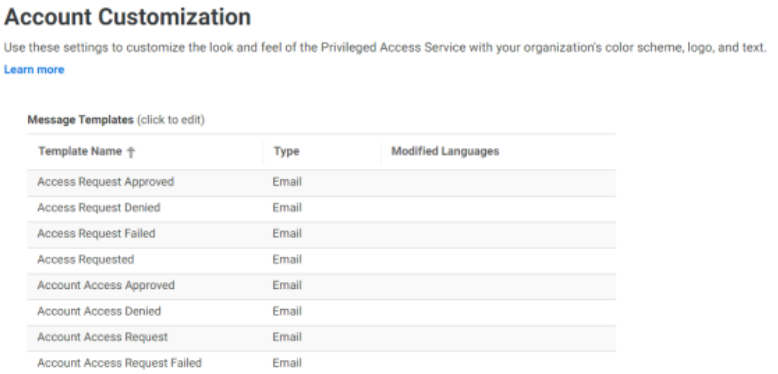
1. Click **Access > Requests**.
2. Select a request from the list to display its details.
3. Click the Actions menu, then click **Delete**.
4. Click **Yes** to confirm that you want to proceed with deleting the request.

Customizing Account Workflow Notification Email

Templates are provided for email notification that is sent when account access is requested, approved, rejected, or cannot be processed. You can use the email templates as-is, or you can customize them.

To customize account workflow notification email:

1. Open the Admin Portal, click **Setting**, then **General**, then click **Account Customization**.
2. Scroll to locate the **Message Customization** section.
3. Select any of the following message templates to customize the content for access requests:



4. For more information about customizing message templates, see How to customize email message contents.

Managing Application Access Requests

In most cases, you give users access to applications by assigning them to one or more specific roles. You can also selectively define a “request and approval” workflow that gives specific users or members of specific roles the ability to approve or reject access requests for specific applications. You can configure the “request and approval” workflow for any of the individual web applications for which you want to manage access requests.

By defining a workflow, users can request access to an application and, if their request is approved, be added to a role with access privileges and see their new application available when they log on to the Admin Portal. A designated “approver” might be a specific user or any member of a specific role. If you configure a role as an approver, the first member to respond to the request is given the authority to approve or reject the request.

Configuring a Request and Approval Workflow

As a member of the sysadmin role or a role with the Role Management administrative right, you can configure roles for all other users. Initially, only the members of the sysadmin role have the ability to enable a “request and approval” workflow and can configure the workflow for selected applications, specify the users or roles with

authority to approve access requests, and identify the role or roles to which users will be assigned if their request is approved.

At a high level, the steps involved in configuring a workflow are these:

- Create one or more roles that can enable a “request and approval” workflow.
- Create one or more roles that can approve access requests for the applications that have a “request and approval” workflow.
- Select an application and click **Workflow** to select the role into which requesters who are approved will be placed.
- Select the user or role with authority to approve requests.

If the Requestor’s Manager is the only approver in the approver list and the user has no manager, the request will be approved. If this is not desirable, verify that your users have a manager (refer to Adding Privileged Access Service users for more information) or add other users or roles to the approver list.

Creating Roles for Workflow Administration

The first few steps in configuring the “request and approval” workflow are optional and involve creating one or more roles for users who are allowed to define a “request and approval” workflow for applications and the roles that can approve access requests. These steps are optional because you can choose to only allow members of the sysadmin role to be the users permitted to configure a workflow and members of the sysadmin role can assign approval authority to individual users without creating any approval roles. In most cases, however, creating roles for different sets of users provides greater flexibility and helps to reduce the number of requests left pending an approval.

If you don’t create any intermediary roles with the appropriate administrative rights to enable a workflow, only members of the sysadmin role will be able to configure any “request and approval” workflow you might want to implement.

In most cases, if you are configuring a request and approval workflow for applications, you should create at least one role for users who are allowed to add, modify, or remove applications and who have permission to change which roles are assigned to a specific applications. If you don’t create a role with the Application Management and Role Management rights, only members of the sysadmin role can configure the “request and approval” workflow for applications.

To configure roles that can enable a workflow

1. Log in to Admin Portal.
2. Click **Access > Roles**.
3. Click **Add Role** or select an existing role to display the role details.

   If you are creating a new role, you must provide at least a unique name for the role.
4. Click **Members**, then click **Add**.
5. Type a search string to search for and select users and groups for this role.
6. Click **Administrative Rights**, then click **Add**.
7. Select the appropriate rights, then click **Add**.

For example, if you are creating a role with permission to enable a workflow for access to applications, select Application Management and Role Management. You can select any additional rights you want included in this role, but you must select at least one of the required administrative rights.

8. Click **Save** to save the role.

Creating Roles for Approvers

You can assign approval authority to individual users. However, in most cases, creating “approver” roles for different sets of users provides greater flexibility and helps to reduce the number of requests left pending an approval. If you don’t create any intermediary roles with the appropriate administrative rights to approve access requests, only members of the sysadmin role will be able to approve access requests. You can follow the same steps described in "Creating Roles for Workflow Administration" on the previous page to create roles for approvers.

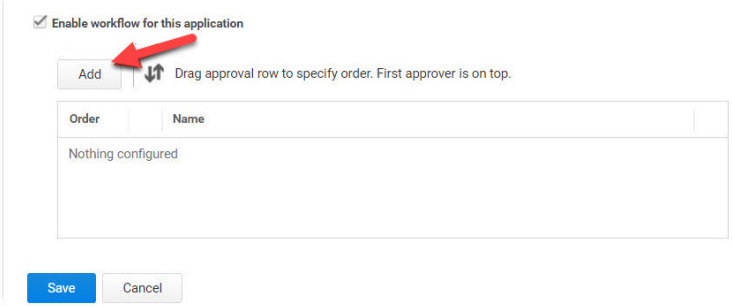
Keep in mind that if you are creating a role with permission to approve access requests for applications, you should include the Application Management and Role Management rights. You can select any additional rights you want included in this role.

Configuring Workflow

As a member of the sysadmin role or a role with Application Management and Role Management administrative rights, you can configure a request and approval workflow for any application.

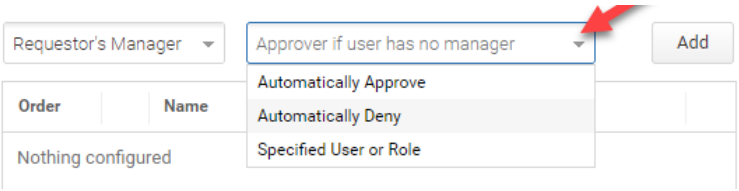
To configure Workflow for applications

1. In Admin Portal, click the **Apps** tab, then select a specific application for which you want to configure a request and approval workflow.
2. Click **Workflow**, then select **Enable workflow for this application**.



3. Click **Add** (above) and select an **Approver Type** from the list (below).

Note: If you choose Requestor’s Manager, you will also need to choose an option for how to handle the request if the user has no manager:



4. Click **Add** again to finish adding the approver type to the list.
5. If you want to have more than one approval before access to the app is granted, repeat the previous two steps.

   Adding steps can be repeated as many times as desired to reflect the required steps in your approval process.

   Note: When multiple approval steps are added, approval is needed from all listed approvers before access is granted. A rejection at any level results in the request being rejected. If the requester's manager is not known, the request proceeds to the next step as though it had been approved. The next approver in the list is notified that the manager was not known, and therefore there has not yet been any approval or rejection of the request.

   Note: The first approver is the only one who can choose which role the user is added to.

   Note: If the manager is the first approver and the requester does not have a manager, the requester will be placed into the first role in the role list if the app request is approved.
6. Click **Save**.

   After you have configured the workflow for an application, users can request access to the application through the Admin Portal.

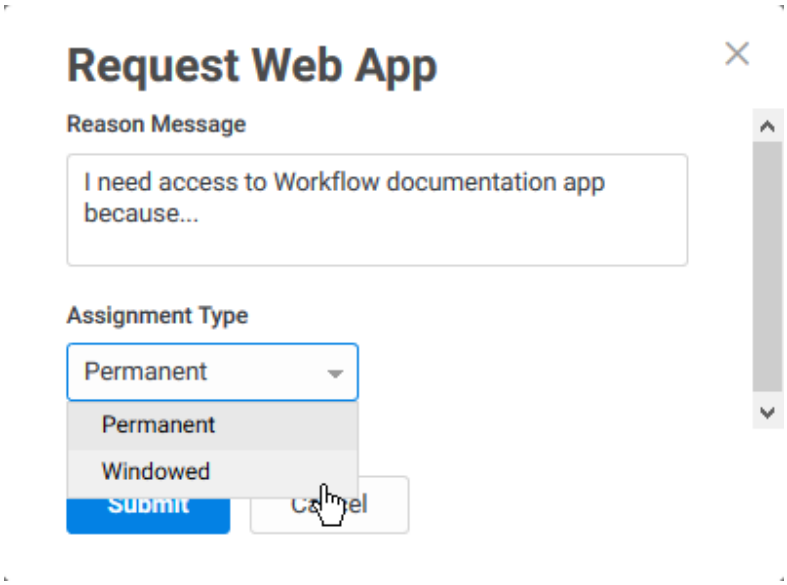
Requesting Access to an Application

Any user who has an account in Privileged Access Service can request access to applications with workflow enabled. No special privileges are required to make requests or approve requests.

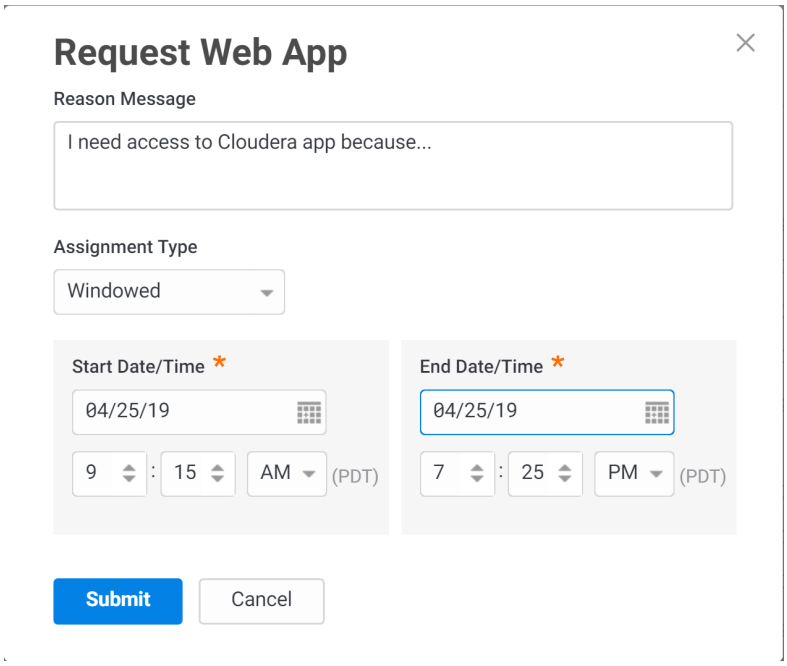
To request access to an application

1. Log on to the Admin Portal.
2. Click **Apps > Add Web Apps**.
3. Type a search string to find the application of interest in the catalog, then right-click or select the check box next to the application.
4. Select **Request Launch** from the Actions menu.

   Only applications with workflow enabled display a Request Launch option.
5. Select either **Permanent** or **Windowed** in the Assignment Type drop-down menu.
   - Permanent - if the request is granted, the user will have access to the app for an indefinite time period, or until it is revoked by an administrator.
   - Windowed - if the request is granted, the user will have access to the app for the specified window, or until it is revoked by an administrator.



6. (Optional) Select the start and end date and time if the request is for a windowed assignment type.



7. Type the business reason for requesting access to the application, then click **Submit** to continue.
8. Click **Close** to close the App Catalog.

   An email notification of your request is sent directly to the designated approver. You can click the Requests tab to see the status of your request. You will also receive an email notification when you request is approved or rejected. If your request was approved, the email will include a link to open the Admin Portal.

Viewing Request Status and History

You will only see the Requests tab if you have made a request or approved a request. After you have made or responded to at least one request, you can click the Requests tab to view the status of requests and the history of request activity.

The list of requests includes the following information:

- **Description** provides a brief summary of the request indicating the type of access or application requested.
- **Status** displays the current status of the request as Pending, Approved, Rejected, or Failed.

  You can review the request details to see the reason the request failed. For example, a request might fail if the email address for the approver or requester is invalid. A failed request might also indicate that the time allowed for taking the requested action has expired. For example, assume the request was for permission to use the root account to log on to a resource and the request was approved with a duration of 60 minutes. If the requester did not log on within 60 minutes of the request approval, the request status will display **Failed**.
- **Posted** displays the date and time of the most recent activity for each request.
- **Approver** displays the user or role designated for approving access requests if the approval is pending or the specific user who approved or rejected the request if the request has been resolved.
- **Requester** displays the user who submitted the request.
- **Latest Log Entry** displays the most recent information recorded for the request.

Viewing Request Details

You will only see the Requests tab if you have made a request or approved a request. After you have made or responded to at least one request, you can click the Requests tab to view the status of requests and the history of request activity.

If you are an approver, you can also go directly to Request Details by clicking the link in the email notifying you of the request.

Regardless of the entry point for viewing request details, the request information table displays details appropriate for the current state of the request. For example, you might see the following information:

- Posted displays the date and time of the most recent activity for each request.
- Description provides a brief summary of the request indicating the type of access or application requested.
- Requester displays the user who submitted the request.
- Requesters Reason displays the business reason provided by the user who submitted the request.
- Approver displays the user or role designated for approving access requests if the approval is pending or the specific user who approved or rejected the request if the request has been resolved.
- Status displays the current status of the request as Pending, Approved, Rejected, or Failed.

  Depending on the status of the request, you might see the reason the request was rejected or the reason why the request failed.

Responding to Application Access Requests

There are no special privileges required to respond to requests. Anyone with access to the Privileged Access Service can be designated as an approver.

If you have been designated as an approver for requests, you will receive an email notification when requests are received. You can click the **View Request** link in the email to view the request details. If you are authorized to approve the request and the request is still pending a response, the Request Details displays the options to Approve or Reject the request.

- Click **Approve** to approve the request and add the requester to the role selected for user access when the "request and approval" workflow was configured. If you click OK to continue with the approval, the request details are updated with the date and time the request was resolved and the approved status.
- Click **Reject** to reject the request and type the reason you are rejecting the request. If you click OK to continue with the rejection, the request details are updated with the reason the request was rejected, the date and time the request was resolved, and the rejected status.

After you respond to the request, the Requests tab is also updated with the latest activity and email is sent to the requester as notification of your response to the request.

To respond to Application Access Requests

1. Access the request details by clicking **View Request** in the email notification or selecting **Access > Requests** and then clicking the request in the Admin Portal.

   The Approve Request window appears.

2. Click either **Approve** or **Reject** to respond to the request.

   Approve

   Reject

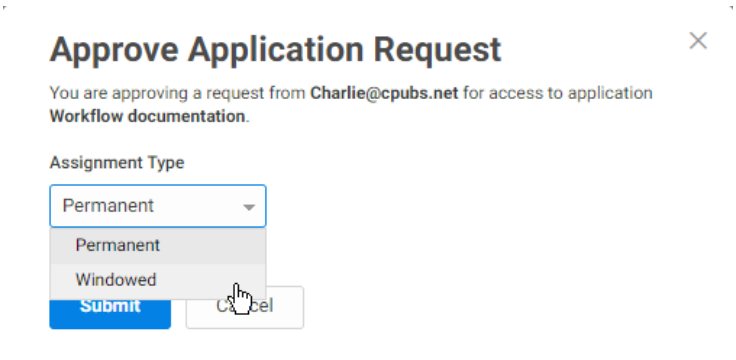
   a. Click **Approve** to approve the request and grant the requester the necessary permissions to the object.

      The Approve Request window appears.

   b. Select either **Permanent** or **Windowed** in the Assignment Type drop-down menu.

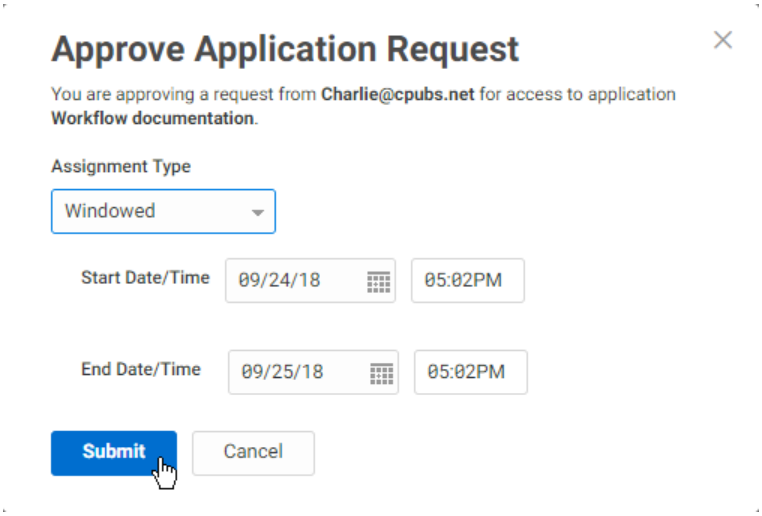
      i. Permanent - Grants the user access to the app for an indefinite time period, or until you revoke access.

      ii. Windowed - Grants the user access to the app for the specified window, or until you revoke access.



c. (Optional) Select the start and end date and time if the approval is for a windowed assignment type.

You can select a windowed approval regardless of the assignment type requested by the user. For example, you can approve access for a windowed time period if the user requested permanent access, or you can change the time window if the user requested windowed access.



d. Click **Submit**.

The request details are updated with the date and time the request was resolved and the approved status.

Click **Reject** to reject the request and type the reason you are rejecting the request. If you click **Submit** to continue with the rejection, the request details are updated with the reason the request was rejected, the date and time the request was resolved, and the rejected status.

Using Agent Auth Workflow

Workflow for AgentAuth provides a user who has only view permission on a system to request Agent Auth access. Once the request is made, one or more approvers indicate whether the request is granted. If granted, the permissions on the system are updated to give the user access. The following sections detail how to use the global Agent Auth workflow:

1. Enabling Agent Auth workflow.
2. Requesting Agent Auth access.
3. Agent Auth access request process.
4. AgentAuth access permissions.

Enabling Agent Auth Workflow

You can enable Agent Auth workflow one of two ways: globally for all systems or locally on the system level.

Enabling Global Agent Auth Workflow

Workflow may be enabled at a global level by navigating to **Settings** > **Resources** > **Agent AuthWorkflow** and checking the **Enable Workflow for all Systems** checkbox.

Enabling Login Workflow on an Individual System

Workflow may be enabled at a system level by navigating to **Resources** > **Systems**. Select and existing system and navigate to **Workflow**. Check the **Enable AgentAuthWorkflow** checkbox.

The approvers may be:

- the user's manager.
- a specific user.
- a role.

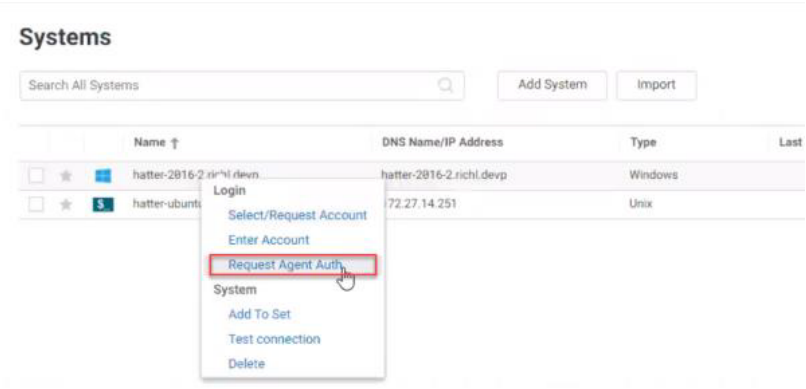
Once enabled, anyone who has view access to a system may request Agent Auth access through workflow. More than one approver may be specified. As such, each approver, in turn, must approve the request. By default, the global workflow settings apply to all systems. An an individual system, however, may specify that Delinea PAS:

- Use the global setting - this is the default settings.
- Override the global setting to disable workflow for this system.
- Override the global setting to enable workflow, specifying a set of approvers that apply only to this system.

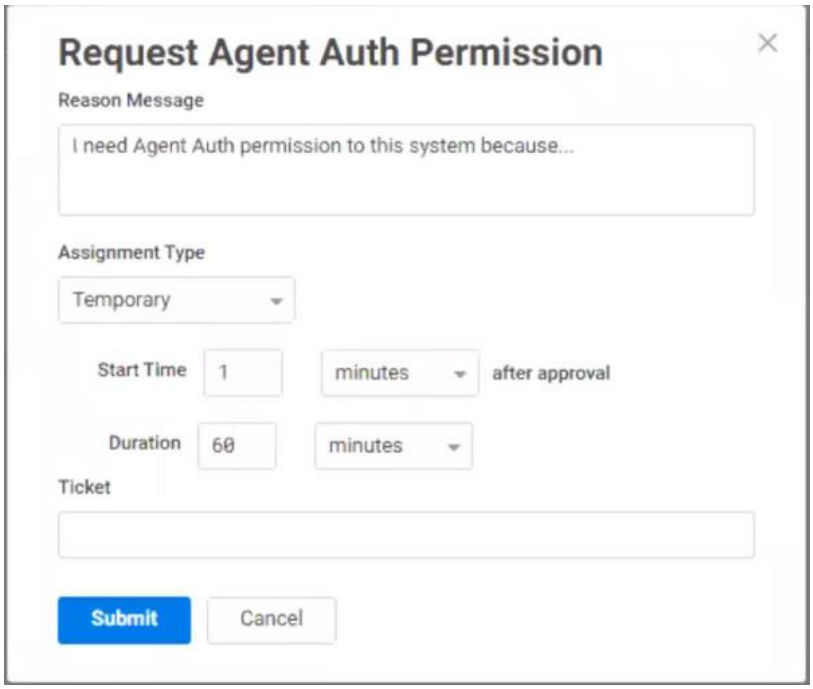
For more information on enabling global Agent Auth workflow, see Configuring global Agent Auth workflow.

Requesting Agent Auth Access

Once Agent Auth is enabled, users with View access on an enrolled system with no permanent Agent Auth access may right-click on a system select **Request Agent Auth Access** on a system as seen below.



and you will see the Agent Auth request screen:



whereby you can make the following settings and click **Submit**.

- Reason Message.
- Assignment Type.
- Start Time after approval.
- Duration.
- Ticket.

Agent Auth Access Request Process

Once the request is submitted, the following occurs:

An Email is Sent to the First Approver

An email is sent to the first approver indicating that an Agent Auth request is pending, the email includes:

- System name.
- Ticket.
- Requestor.
- Reason for the ticket.
- Approver 1 name and email address.
- A link to the request in the PAS Admin Portal.

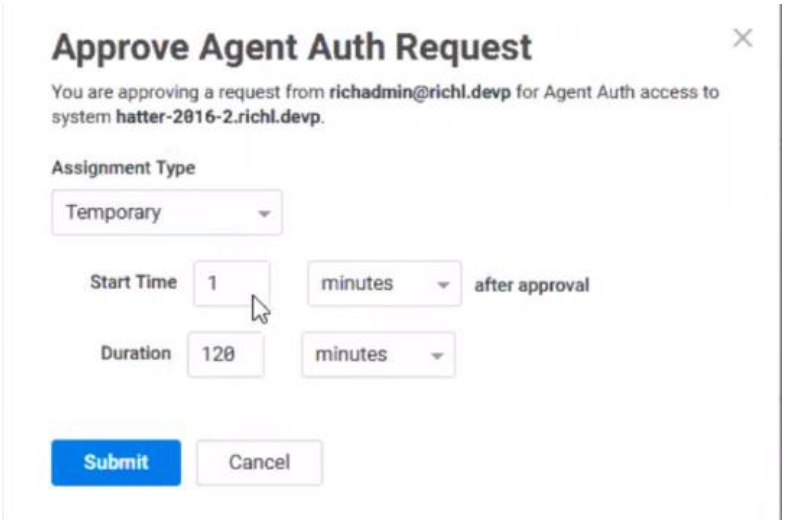
The Request Appears in the Approver's PAS Instance

The request appears in the approver's Admin Portal under: **Access** > **Requests** with the following information:

- Request post date and time.
- Request description - includes name and folder of the system secret.
- Requested system.
- DNS Name.
- Ticket.
- Requestor.
- Requestor reason.
- Approver 1 email address.
- Status.
- Latest log entry for the workflow.

Approving or Rejecting an Agent Auth Workflow

1. To approve or reject a workflow request, you can either follow the link from the request email or navigate to the Admin Portal > **Access** > **Requests**. Here, you can do the following:
   - **Approve**: The first approver may adjust access request (temporary, permanent, or windowed) and start/end times of temporary and windowed requests:



   - **Reject**: specify a reason the request is denied.

   Note: If there is more than one approver, the next approver on the list is sent an email as described above and they can approve or reject the request. If an approver is a role, any member of the role may approve/reject.

2. The request is copied to the requestor's and approver's Admin Portal under **Access** > **Request**.

Approval and Rejection Email Information

The following information is included in approval and rejection emails:

Approval email: when the final approver approves a request, an email is sent to the requester with the following:

- System name.
- Ticket.
- Assignment details:
  - For temporary and windowed assignments: the start/end time (which may have been adjusted from original request).
  - For permanent assignments: assignment type.
  - List of persons who approved and rejected the request.

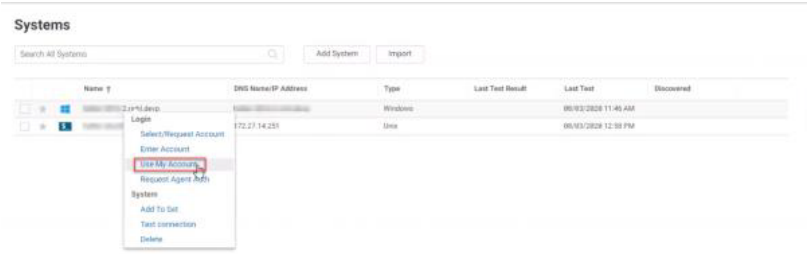
Rejection email: When any approver rejects a request, an e-mail is sent to the requestor with the following:

- System name.
- Ticket.
- List of persons who approved and rejected the request.
- Reason for rejection.
- A link to the request.

Agent Auth Access Permissions

If approved, you will have the following permissions with Agent Auth workflow:

- The AgentAuth access right is added to the **System** / <system> / **Permissions** tab. The permissions list has **Starts** and **Expires** columns to indicate a windowed assignment of permission.
- The requester is permitted to use the AgentAuth to login to the system directly using his or her account or may **Use My Account** (as seen below). As with any other permission, the administrator may remove the permission assignment at any time.



Enabling Auditing for Remote Sessions

All components of the Privileged Access Service log audit trail events for the activity on systems, domains, databases, applications, and accounts that you add to the service. If you also want to audit user session activity

initiated from the Admin Portal on target systems, you can enable the auditing and monitoring services that are part of the Privileged Access Service enterprise offering.

To prepare for auditing, you must have at least one working audit installation running in your environment. If you don't have an audit installation and want to create one, you can download the auditing and monitoring services for Privileged Access Service from the Customer Support Portal, then follow the instructions in the *Auditing and Monitoring Administration* to set up a working environment.

The audit installation must include the following core components:

- A management database to store installation information
- The audit store and audit store database to define the scope and store session activity
- At least two collectors to collect session activity and send it to the audit store database
- The Audit Manager console to manage installation components, audit roles, and permissions
- The Audit Analyzer console to view, query, and manage recorded activity

For information about creating the audit installation and configuring the core components of the installation, see the *Auditing and Monitoring Administration*.

If you are familiar with auditing using the auditing infrastructure, you might have an agent installed on some or all of your target systems. However, the agent is not required to audit session activity on the remote target computers you have added to the Privileged Access Service. Instead, you can use the Cloud Connector to send session activity directly to the collector without installing an agent or the auditing service on the target system. The only additional requirement to enable auditing using the connector is that the computer you are using for the connector must be within the scope of an audit store—that is, the computer must be included in the site, subnet, or IP address identified as the audit store. The session activity for all target systems will be sent to the audit store that includes the computer where the connector is installed.

For more information about defining the scope for an audit store, see the *Auditing and Monitoring Administration* or Creating the First Audit Store. If you're working with systems inside of a DMZ, be sure to read Auditing systems that are inside a DMZ.

Auditing Sessions on Target Systems

All of the administrative activity that takes place through the Privileged Access Service is audited and stored as events either locally or in the Privileged Access Service. In addition, if you have installed auditing services and have an audit installation established, the administrator's activity on the target system during a secure shell or remote desktop session can also be collected and stored in an audit database for further review and analysis.

Capturing and Replaying Sessions

If you have an audit installation available and enable auditing, the connector captures all of the secure shell and remote desktop activity in the sessions you open from the administrative portal. The connector sends the recorded sessions to the collector service, which forwards the sessions to the audit store database. You can play back the recorded sessions using Audit Analyzer. You can also use Audit Analyzer to create queries and reports based on session activity and to review, update, or delete the sessions.

If you have multiple connectors, the connector used to record the session is selected randomly when you start the SSH or RDP session. If the connector with an active session stops running, the session is disconnected. If the

connector is recording a remote desktop session when it stops, you can manually reconnect to the target system using a different connector to resume the session. However, the session segments are recorded in the audit store database as two separate audit sessions. The connector will spool audited session activity if it can't connect to any collectors.

You must have the required Privileged Access Service components installed to audit the sessions you open from the Admin Portal. If you have an older version of Server Suite, you must upgrade before enabling auditing using the connector.

For more information about managing the audit installation, querying and reviewing session activity, and other auditing-specific topics, see the *Auditing and Monitoring Administration*.

Windows Sessions Recorded by a Connector

If you are already auditing session activity on Windows computers, you might notice a few differences between sessions recorded directly on a Windows computer that has an agent installed and the remote desktop sessions recorded by the Cloud Connector. For example, if a Windows session is recorded by the connector, you might notice the following differences:

- Windows sessions recorded by the connector do not include an indexed list of events.
- You cannot specify any agent configuration settings, such as the color depth to use or the offline data storage location.
- There is no role-based auditing or integration to skip auditing for some activity or to audit only privileged activity.
- Windows sessions recorded by the connector do not include any information about the DirectAuthorize desktop being used or about desktop changes.

  However, you can use the desktop label to determine the desktop used for different operations when replaying Windows sessions.

UNIX Sessions Recorded by a Connector

If you are already auditing session activity on UNIX computers, you might notice a differences between sessions recorded directly on a Linux or UNIX computer that has an agent installed and the remote shell sessions recorded by the Centrify Connector. For example, if a UNIX session is recorded by the connector, you might notice the following differences:

- UNIX sessions recorded by the connector do not include standard input (`stdin`).
- You cannot specify any agent configuration settings that you control using the `centrifyda.conf` file, such as password masking.
- There is no role-based auditing or integration to skip auditing for some activity or to audit only privileged activity.
- You cannot configure "per command" auditing.
- You cannot obfuscate any sensitive information that might be captured in a session.

Specifying the Audit Installation

After you have created an audit installation and verified you have a working environment, you can enable auditing and specify the installation name for the systems you manage in the Admin Portal.

To configure auditing settings:

1. In the Admin Portal, click **Settings** > **Resources** to display the settings available for Privileged Access Service.
2. Click **DirectAudit**.
3. Select **Enable Auditing**.
4. Type the name of the audit installation where you want to audit user activity on the systems you manage.
5. Optionally, click **Add** to map one or more connectors to a specific audit installation.

   If you have multiple audit installations—for example, to support multiple data centers— you might want to specify which connectors to use for each audit installation for network efficiency, high availability, and load balancing.

   After clicking Add:

   - Specify an audit installation name.
   - Select one or more connectors from the list of available connectors to receive and transfer audited activity.
   - Click **Done**.
6. Click **Save** to save the setting.

Adding Connectors to a Secure Installation

If you have configured auditing to run as a secure installation that only allows agents to connect to trusted collectors and collectors to only accept connections from trusted agents, you must add the connectors you are using to the list of trusted audited systems for the audit store. If the connectors are not identified as trusted systems, the sessions and audit trail events captured by the connector will not be accepted by the audit store database.

For information about configuring a secure installation and how to identify trusted systems, see the *Auditing Administrator's Guide*.

Downloading the Audit Packages for the Cloud Clients

In order to enable full auditing on a system outside of Active Directory, please download and install the following audit packages, depending on your system:

Windows: After enrolling the system with the Cloud Client for Windows, download and install the Windows - Audit package. The audit package enables the system for auditing.

Linux: After enrolling the system with the Cloud Client for Linux, download the two additional audit packages appropriate for your Linux system. Install these Linux audit packages in the following order:

1. <Linux operating system> - OpenSSL
2. <Linux operating system> - Audit

For more information about configuring your audit installation to collect data from non-Active Directory systems, see Checklist for auditing systems outside of Active Directory.

Audit Commands Included with the Cloud Client for Windows Audit Package

If you install the audit package and enable auditing for a system that has the Cloud Client for Windows installed, you can use any of the following commands with the `caudit.exe` command line program to enable or disable auditing,

display audit status, or change the log level. You must have local administrative rights to enable or disable auditing, change the log level, or prepare a diagnostics package.

Caudit Option	Description
`-e, --enable`	Enable auditing on the system enrolled in Centrify PAS.
`-d, --disable`	Disable auditing on the system enrolled in Centrify PAS
`-i, --info`	Display current audit status and diagnostics information.
`-l, --loglevel`	Set the log level and exit. You can set the log level to any of the following: TRACE, DEBUG, INFO, WARN, ERROR, DISABLED
`-t, --support`	Prepare diagnostics package for technical support.
`-v, --version`	Print version information and exit.
`-h, --help`	Print this help information and exit.

Auditing Systems Outside of Active Directory

You can use gateway-based auditing for systems that are not in your Active Directory system. For the non-Active Directory systems that you need to audit, you have two ways to do so:

- (Option A) Install and enroll the Cloud Client on the systems you want audit.
- (Option B) Configure your non-Active Directory cloud connectors to point to your audit collectors (which are joined to Active Directory). Any systems connected to PAS by way of these cloud connectors will be audited.

For option A, the details of what you need to do are specified in Checklist for auditing systems outside of Active Directory.

For option B, follow just steps 1-6 in the Checklist for auditing systems outside of Active Directory, and then configure your non-Active Directory cloud connectors with the changes below.

To configure a non-Active Directory cloud connector to point to your Active Directory-joined audit collectors:

- Make the following registry key changes:

```
  Location - HKLM\\SOFTWARE\\Centrify\\Cloud
   Name - NGDACollectorsOverride
   Type - REG_MULTI_SZ
   Value - One or more collectors in FQDN:Port format. For example,
DACOLLECTORHOST1.ACME.COM:5064.
```

Note: Port 5064 is the default value; be sure to use the same port that your audit collectors use. You can open the Collector Control Panel to see which ports that the audit collectors are using.

You can make the registry key changes at the command line by running a command with the following syntax:

```
reg.exe add HKLM\\SOFTWARE\\Centrify\\Cloud /v NGDACollectorsOverride /t
REG_MULTI_SZ /d <one or more collector hosts in FQDN:Port format separated by
\\0\>
```

Here's an example:

```
reg.exe add HKLM\\SOFTWARE\\Centrify\\Cloud /v NGDACollectorsOverride /t
REG_MULTI_SZ /d DACOLLECTORHOST1.ACME.COM:5064\\0DACOLLECTORHOST2.ACME.COM:5064`
```

Export Data using Delinea Escrow Functions

The following commands are available for exporting and emailing data attributes for Systems, Accounts, Domains, and Databases from Privileged Access Service:

Command	Description
Set-EscrowKey -Endpoint -Token -FilePath	Uploads the public key to the Admin Portal and stores it in the tenant configuration.
Set-EscrowEmail -Endpoint -Token -Emails	Configures the recipients that will receive the email containing the Systems, Accounts, Domains, and Database data and stores it in the tenant configuration. Separate multiple email recipients using one of the following: , ; space.
Get-EscrowEmail -Endpoint -Token	Displays email addresses for recipients designated to receive the exported content.
Run-Escrow -Endpoint -Token	Exports the data for Systems, Accounts, Domains, and Databases. Securely sends the .csv file to designated email recipients. If the amount of data before encryption and compression exceeds more than 20MB, the additional data is written to another file and sent in a second email. A passphrase is required in order to open the attachments in the email.
Schedule-Escrow -Endpoint -Token	Sets the escrow job (exports data) to run every 24 hours. To change the default configuration, you use CPS.EscrowJobIntervalTimeSpan. The time span is entered as days, hours, minutes, and seconds (d.hh:mm:ss or hh:mm:ss). For example, entering 2.08:30:10 indicates data will be exported every 2 days 8 hours 30 minutes and 10 seconds.

Command	Description
Unschedule-Escrow -Endpoint -Token	Cancels the schedule for the escrow job (data export).
Get-EscrowScheduleStatus -Endpoint -Token	Displays whether a schedule for exporting data is configured to run periodically (default is every 24 hours). Returns a value of True (schedule is configured) or False (schedule is not configured).

To Export Data Using Delinea Commands in PowerShell:

Depending on the number of entities you are exporting, the process might take some time to complete.

1. Verify that the computer you are using to export data has access to the Privileged Access Service Admin Portal and that the user to be logged in tothe Admin Portal has the System Administrator role (defined in the Admin Portal).
2. Open the Centrify.Samples.PowerShell.Example.ps1 script file you downloaded earlier to use as a template to run the commands.
3. Modify the script file (uncomment the appropriate lines) to run commands in order to export the data attributes for Systems, Accounts, Domains, andDatabases from Privileged Access Service and email it to designated recipients.

   At a minimum you must run the following commands (uncomment the command lines) to export the data and email it to recipients:

   - Set-EscrowKey -Endpoint -Token -FilePath
   - Set-EscrowEmail -Endpoint -Token -Emails
   - Run-Escrow -Endpoint -Token
4. Start Windows PowerShell to open a command window and run the modified script (Delinea.Samples.PowerShell.Example.ps1).

   The script calls the Centrify.Samples.PowerShell.Example.ps1 module to export Systems, Domains, Databases, Accounts and their attributes into a CSV file and emails it to designated recipients.

Exporting Data using Escrow Functions

Users with the System Administrator role can securely export encrypted data attributes including account passwords for Systems, Accounts, Domains, and Databases from Privileged Access Service using Centrify commands and the Escrow PowerShell module. The data exported is aggregated into a CSV file, similar to the import Sample.csv template described in Importing systems, accounts, domains, databases.

The exported data can be securely emailed to designated recipients using the PGP encryption program. If the amount of data before encryption and compression exceeds more than 20MB, the additional data is written to another file and sent to recipients in a second email. To open the email attachment that contains the data, you need to enter a passphrase to unlock the OpenPGP secret key.

Note: The data from the exported file can be imported back into Privileged Access Service (see Importing systems, accounts, domains, databases).

To download the export escrow script and install the PGP program:

1. Access Github at https://github.com/centrify/centrify-samples-powershell to download the following escrow script files to your local computer.
   - Privileged Access Service PowerShell script (Centrify.Samples.PowerShell.Example.ps1)
   - The script can be used as a template to run the commands.
   - Privileged Access Service PowerShell Escrow module (Centrify.Samples.PowerShell.CPS.Export.psm1)
   - The module file is called from the CentrifyPowerShell script and does not require any modification. To import the module you also need https://github.com/centrify/centrify-samples-powershell/module/Centrify.Samples.PowerShell.psm1.
2. Get a PGP encryption key pair using a PGP key generator and export the public key to your local computer. For more information see, https://www.openpgp.org/software/.

- The encryption key is used to encrypt the data before emailing the data to designated recipients.

3. Once you have the script files and the encryption keys, export the data and email it to designated recipients (see "Exporting Data using Escrow Functions").

Export Data Using Centrify Escrow Functions

The following commands are available for exporting and emailing data attributes for Systems, Accounts, Domains, and Databases from Privileged Access Service:

Command	Description
Set-EscrowKey -Endpoint -Token -FilePath	Uploads the public key to the Admin Portal and stores it in the tenant configuration.
Set-EscrowEmail -Endpoint -Token -Emails	Configures the recipients that will receive the email containing the Systems, Accounts, Domains, and Database data and stores it in the tenant configuration. Separate multiple email recipients using one of the following: , ; space.
Get-EscrowEmail -Endpoint -Token	Displays email addresses for recipients designated to receive the exported content.
Run-Escrow -Endpoint -Token	Exports the data for Systems, Accounts, Domains, and Databases. Securely sends the .csv file to designated email recipients. If the amount of data before encryption and compression exceeds more than 20MB, the additional data is written to another file and sent in a second email. A passphrase is required in order to open the attachments in the email.

Command	Description
Schedule-Escrow -Endpoint -Token	Sets the escrow job (exports data) to run every 24 hours. To change the default configuration, you use CPS.EscrowJobIntervalTimeSpan. The time span is entered as days, hours, minutes, and seconds (d.hh:mm:ss or hh:mm:ss). For example, entering 2.08:30:10 indicates data will be exported every 2 days 8 hours 30 minutes and 10 seconds.
Unschedule-Escrow -Endpoint -Token	Cancels the schedule for the escrow job (data export).
Get-EscrowScheduleStatus -Endpoint -Token	Displays whether a schedule for exporting data is configured to run periodically (default is every 24 hours). Returns a value of True (schedule is configured) or False (schedule is not configured).

|

To export data using Centrify commands in PowerShell:

Depending on the number of entities you are exporting, the process might take some time to complete.

1. Verify that the computer you are using to export data has access to the Privileged Access Service Admin Portal and that the user to be logged in to the Admin Portal has the System Administrator role (defined in the Admin Portal).
2. Open the Centrify.Samples.PowerShell.Example.ps1 script file you downloaded earlier to use as a template to run the commands.
3. Modify the script file (uncomment the appropriate lines) to run commands in order to export the data attributes for Systems, Accounts, Domains, and Databases from Privileged Access Service and email it to designated recipients.

- At a minimum you must run the following commands (uncomment the command lines) to export the data and email it to recipients:
  - Set-EscrowKey -Endpoint -Token -FilePath
  - Set-EscrowEmail -Endpoint -Token -Emails
  - Run-Escrow -Endpoint -Token

4. Start Windows PowerShell to open a command window and run the modified script (Centrify.Samples.PowerShell.Example.ps1).

- The script calls the Centrify.Samples.PowerShell.CPS.Export.psm1 module to export Systems, Domains, Databases, Accounts and their attributes into a CSV file and emails it to designated recipients.

-->

CSV File Data Attribute Fields

The following table describes the fields in the CSV output file.

For this template field	The following information is displayed
Entity Type	Includes one of the following entity types:- System- Domain- Database- Account
Name	The name of the system, domain or database exported. You can have multiple lines with the same name. For example, if you exported more than one account for the same system, each account is listed as a separate line with the same system name. Applies to Systems, Domains, and Databases.
FQDN	Fully-qualified domain name or IP address of the System or Database you want to add. This field applies to Systems and Databases.
Description	Descriptive information added for the entity. This field applies to Systems, Domains, Databases, and Accounts.
ComputerClass	One of the following values for the type of system added:- Windows- Unix- GenericSsh- Cisco AsyncOS- CiscoIOS- CiscoNXOS- JuniperJunos- HPNonStopOS- IBMi- CheckPointGaia- PaloAltoNetworksPANOS- F5NetworksBIGIP- VMwareVMkernel This field is required and applies to Systems.
ProxyUser	The name of the “proxy” user for a system. This field is optional and applies to Systems.- For more information about the “proxy” user for Windows systems, see the following topic: Configuring a proxy user for password operations- For more information about the “proxy” user for UNIX and Juniper systems, see the following topic: Specifying a proxy account for root
ProxyUserPassword	The password for the “proxy” user for a system. This field is optional and applies to Systems. - For more information about the “proxy” user for Windows systems, see the following topic: Configuring a proxy user for password operations - For more information about the “proxy” user for UNIX and Juniper systems, see the following topic:Specifying a proxy account for root
ProxyUserIsManaged	Whether the password for the “proxy” user is managed. This field is optional and applies to Systems. TRUE indicates the “proxy” account password is managed by Privileged Access Service. FALSE indicates the password is unmanaged.

For this template field	The following information is displayed
ResourceDomain	The domain that the system is joined to. This field is optional and applies to Systems.
ResourceDomainOperationsEnabled	Specify whether you want to use the domain administrative account to enable zone role workflow. You specify TRUE if you want to use the domain administrative account to enable operations such as zone role workflow, or FALSE if you do not want to use the domain administrative account to enable domain operations. In order to enable domain operations for a system, the user must have grant rights over the domain or else the import will fail. This field applies to Systems.
ResourceSessionType	Indicates remote connection type: Ssh for secure shell or Rdp for remote desktop. This field is required and applies to Systems.
ResourceSessionTypePort	The port used for remote connections. The default port for SSH is 22 and for RDP it is 3389. This field applies to Systems.
ResourceWindowsManagementMode	One of the following management modes used to manage the Windows System. Unknown (this is equivalent to auto-detect in the Admin Portal) - Smb WinRMOverHttp - WinRMOverHttps - RpcOverTcp - Disabled This field applies to Systems.
ResourceWindowsManagementPort	The management port to be used for password management for Windows, F5 Networks BIG-IP, and Palo Alto Networks PAN-OS Systems. This field applies to Systems.
PasswordProfile	Customized password profile name to define the rules applied when managed passwords are generated for systems, domains, or databases. For more information about customized password profiles, see Configuring password profiles. This field is applies to Systems, Domains, and Databases.
SetName	Name for system, domain, database, or account sets. Sets are logical groups of a particular type (system, domain, database, or account) to simplify management activity and reporting for entities with attributes in common. For more than one set name for an entity, entries are separated by a |. For example, SystemSet1|SystemSet2|SystemSet3. This field applies to Systems, Domains, Databases, and Accounts.

For this template field	The following information is displayed
DefaultCheckoutTime	The length of time (in minutes) that a checked out password is valid. The minimum checkout time is 15 minutes. If no value is specified, the default is 60 minutes. Also see, Setting systemspecific policies. This field applies to Systems, Domains, Databases, and Accounts.
AllowRemote	TRUE (allows remote connections from a public network for a selected system) or FALSE (does not allow remote connections from a public network).</br/br>This field is optional and applies to Systems.
ParentEntityTypeOfAccount	Entity type related to the account (System, Domain or Database). This field applies to Accounts.
ParentEntityNameOfAccount	Display name of the system, domain or database associated with the account. This field applies to Accounts.
User	User name for an account used with Systems, Domains, and Databases. This field applies to Accounts.
Password	The password for the account used with the system. This field is optional and applies to Accounts.
IsManaged	TRUE if Privileged Access Service manages the password for the account, or FALSE if the password is unmanaged. This field applies to Accounts.
AccountMode	Expert if an expert mode account exists for Checkpoint Gaia systems. This field applies to Systems.
UseProxy	TRUE if a “proxy” account is used for the system, or FALSE if a “proxy” account for the system is not used. For UNIX and Juniper systems, this field is used if your secure shell environment is configured to not allow the root user to access computers remotely using SSH. This field is also used for Windows systems if you use a proxy account for Windows Remote Management (WinRM) connections to a system. This field applies to accounts.
DatabaseServiceType	One of the following database types: - SQLServer - Oracle - SAP Adaptive Server Enterprise (ASE) This field applies to Databases.
OracleServiceName	The service name assigned to the Oracle database. Also see, Adding databases. This field applies to Databases.

For this template field	The following information is displayed
SQLInstanceName	The instance name assigned to the SQL Server database. Also see, Adding databases. This field applies to Databases.
DatabasePort	The port number used to check the status of the database and when updating database passwords. This field applies to Databases.
ParentDomain	The name of the parent domain, if a child domain is configured. This field applies to Domains.
AdministrativeAccount	The administrative account in the format admin@childdomain, admin@mycompany.com or a local account . This field applies to Systems and Domains.
AllowAutomaticAccountMaintenance	TRUE (allows out-of-sync passwords to be reset and managed accounts to be unlocked during login or checkout), or FALSE (does not allow out-of-sync passwords to be reset and managed accounts to be unlocked during login or checkout). Requires an Administrative Account be defined for the domain. This field applies to Domains.
AllowManualAccountUnlock	TRUE (allows users with the Unlock Account permission to manually unlock accounts), or FALSE (does not allow accounts to be manually unlocked). Requires an Administrative Account be defined for the domain. This field is optional and applies to Domains.
AllowMultipleCheckouts	FALSE (only one user is allowed to check out the password at any given time) or TRUE (allows multiple users to have the account password checked out at the same time without waiting for the password to be checked in). Also see, Allow multiple password checkouts. This field applies to Systems, Domains, and Databases.
AllowPasswordRotation	TRUE (Privileged Access Service rotates managed passwords periodically) or FALSE (Privileged Access Service does not rotate managed passwords periodically). This field applies to Systems, Domains, and Databases.
PasswordRotateDuration	The interval at which managed passwords are automatically rotated. This field applies to Systems, Domains, and Databases.
MinimumPasswordAge	The minimum number of days before a password is rotated. This field applies to Systems, Domains, and Databases.
AllowPasswordHistoryCleanUp	TRUE (allows periodic password history cleanup), or FALSE (does not allow periodic password history cleanup). This field applies to Systems, Domains, and Databases.

For this template field	The following information is displayed
PasswordHistoryCleanUpDuration	The number of days after which retired passwords matching the duration are deleted. This field applies to Systems, Domains, and Databases.

CSV File Data Attribute Fields

The following table describes the fields in the CSV output file.

For this template field	The following information is displayed
Entity Type	Includes one of the following entity types: System Domain Database Account
Name	The name of the system, domain or database exported. You can have multiple lines with the same name. For example, if you exported more than one account for the same system, each account is listed as a separate line with the same system name. Applies to Systems, Domains, and Databases.
FQDN	Fully-qualified domain name or IP address of the System or Database you want to add. This field applies to Systems and Databases.
Description	Descriptive information added for the entity. This field applies to Systems, Domains, Databases, and Accounts.
ComputerClass	One of the following values for the type of system added: Windows Unix GenericSsh Cisco AsyncOS CiscoIOS CiscoNXOS JuniperJunos HPNonStopOS IBMi CheckPointGaia PaloAltoNetworksPANOS F5NetworksBIGIP VMwareVMkernel This field is required and applies to Systems.
ProxyUser	The name of the “proxy” user for a system. This field is optional and applies to Systems. For more information about the “proxy” user for Windows systems, see the following topic: Configuring a proxy user for password operations For more information about the “proxy” user for UNIX and Juniper systems, see the following topic: Specifying a proxy account for root

For this template field	The following information is displayed
ProxyUserPassword	The password for the “proxy” user for a system. This field is optional and applies to Systems. For more information about the “proxy” user for Windows systems, see the following topic: Configuring a proxy user for password operations For more information about the “proxy” user for UNIX and Juniper systems, see the following topic: Specifying a proxy account for root
ProxyUserIsManaged	Whether the password for the “proxy” user is managed. This field is optional and applies to Systems. TRUE indicates the “proxy” account password is managed by Privileged Access Service. FALSE indicates the password is unmanaged.
ResourceDomain	The domain that the system is joined to. This field is optional and applies to Systems.
ResourceDomainOperationsEnabled	Specify whether you want to use the domain administrative account to enable zone role workflow. You specify TRUE if you want to use the domain administrative account to enable operations such as zone role workflow, or FALSE if you do not want to use the domain administrative account to enable domain operations. In order to enable domain operations for a system, the user must have grant rights over the domain or else the import will fail. This field applies to Systems.
ResourceSessionType	Indicates remote connection type: Ssh for secure shell or Rdp for remote desktop. This field is required and applies to Systems.
ResourceSessionTypePort	The port used for remote connections. The default port for SSH is 22 and for RDP it is 3389. This field applies to Systems.
ResourceWindowsManagementMode	One of the following management modes used to manage the Windows System. Unknown (this is equivalent to auto-detect in the Admin Portal) Smb WinRMOverHttp WinRMOverHttps RpcOverTcp Disabled This field applies to Systems.
ResourceWindowsManagementPort	The management port to be used for password management for Windows, F5 Networks BIG-IP, and Palo Alto Networks PAN-OS Systems. This field applies to Systems.

For this template field	The following information is displayed
PasswordProfile	Customized password profile name to define the rules applied when managed passwords are generated for systems, domains, or databases. For more information about customized password profiles, see Configuring password profiles. This field is applies to Systems, Domains, and Databases.
SetName	Name for system, domain, database, or account sets. Sets are logical groups of a particular type (system, domain, database, or account) to simplify management activity and reporting for entities with attributes in common. For more than one set name for an entity, entries are separated by a |. For example, SystemSet1|SystemSet2|SystemSet3. This field applies to Systems, Domains, Databases, and Accounts.
DefaultCheckoutTime	The length of time (in minutes) that a checked out password is valid. The minimum checkout time is 15 minutes. If no value is specified, the default is 60 minutes. Also see, Setting systems specific policies. This field applies to Systems, Domains, Databases, and Accounts.
AllowRemote	TRUE (allows remote connections from a public network for a selected system) or FALSE (does not allow remote connections from a public network). This field is optional and applies to Systems.
ParentEntityTypeOfAccount	Entity type related to the account (System, Domain or Database). This field applies to Accounts.
ParentEntityNameOfAccount	Display name of the system, domain or database associated with the account. This field applies to Accounts.
User	User name for an account used with Systems, Domains, and Databases. This field applies to Accounts.
Password	The password for the account used with the system. This field is optional and applies to Accounts.
IsManaged	TRUE if Privileged Access Service manages the password for the account, or FALSE if the password is unmanaged. This field applies to Accounts.
AccountMode	Expert if an expert mode account exists for Checkpoint Gaia systems. This field applies to Systems.

For this template field	The following information is displayed
UseProxy	TRUE if a “proxy” account is used for the system, or FALSE if a “proxy” account for the system is not used. For UNIX and Juniper systems, this field is used if your secure shell environment is configured to not allow the root user to access computers remotely using SSH. This field is also used for Windows systems if you use a proxy account for Windows Remote Management (WinRM) connections to a system. This field applies to Accounts.
DatabaseServiceType	One of the following database types: SQLServer Oracle SAP Adaptive Server Enterprise (ASE) This field applies to Databases.
OracleServiceName	The service name assigned to the Oracle database. Also see, Adding databases. This field applies to Databases.
SQLInstanceName	The instance name assigned to the SQL Server database. Also see, Adding databases. This field applies to Databases.
DatabasePort	The port number used to check the status of the database and when updating database passwords. This field applies to Databases.
ParentDomain	The name of the parent domain, if a child domain is configured. This field applies to Domains.
AdministrativeAccount	The administrative account in the format admin@childdomain, admin@mycompany.com or a local account . This field applies to Systems and Domains.
AllowAutomaticAccountMaintenance	TRUE (allows out-of-sync passwords to be reset and managed accounts to be unlocked during login or checkout), or FALSE (does not allow out-of-sync passwords to be reset and managed accounts to be unlocked during login or checkout). Requires an Administrative Account be defined for the domain. This field applies to Domains.
AllowManualAccountUnlock	TRUE (allows users with the Unlock Account permission to manually unlock accounts), or FALSE (does not allow accounts to be manually unlocked). Requires an Administrative Account be defined for the domain. This field is optional and applies to Domains.
AllowMultipleCheckouts	FALSE (only one user is allowed to check out the password at any given time) or TRUE (allows multiple users to have the account password checked out at the same time without waiting for the password to be checked in). Also see, Allow multiple password checkouts. This field applies to Systems, Domains, and Databases.

For this template field	The following information is displayed
AllowPasswordRotation	TRUE (Privileged Access Service rotates managed passwords periodically) or FALSE (Privileged Access Service does not rotate managed passwords periodically). This field applies to Systems, Domains, and Databases.
PasswordRotateDuration	The interval at which managed passwords are automatically rotated. This field applies to Systems, Domains, and Databases.
MinimumPasswordAge	The minimum number of days before a password is rotated. This field applies to Systems, Domains, and Databases.
AllowPasswordHistoryCleanUp	TRUE (allows periodic password history cleanup), or FALSE (does not allow periodic password history cleanup). This field applies to Systems, Domains, and Databases.
PasswordHistoryCleanUpDuration	The number of days after which retired passwords matching the duration are deleted. This field applies to Systems, Domains, and Databases.

Assigning PowerShell remote access

If you want to allow some of your users to be able to run PowerShell commands on remote computers by way of PowerShell remoting, be aware of the following requirements:

- The target computer needs to have the Delinea Client for Windows installed with the Privileged Access Service enabled.
- Assign the user to a role with the "PowerShell remote access is allowed" system right granted.

If you're using the Delinea Audit & Monitoring Service, when a user attempts to run PowerShell remotely on a computer, the system triggers an audit trail event. Delinea Audit & Monitoring Service is an optional service.

To assign PowerShell remote access to a user:

1. In the **Access Manager** console, open the zone that the Windows system to be managed belongs to (Access Manager is not necessarily installed on the machine with the Windows client).
2. Under **Role Definitions**, right-click a role that you'd like to assign PowerShell remote access permission to and select **Properties**.
3. Under **System Rights** > **Windows rights**, select **PowerShell remote access is allowed**.
4. Right-click **Role** > **Assignment** and select **Assign Role**.
5. Select the role as defined above and assign the Windows account to it.

Applications

Applications Use Centrify Application Access and Application Gateway Services to leverage identity to secure administrator's access to apps through single sign-on, multi-factor authentication, and mobility management.

Introduction to Application Management

To deploy web applications, add the application from the Delinea App Catalog, modify the application settings, and assign roles to the application to specify who has access to the application.

Working with applications

"Introduction to Application Management" above"Application Types" on page 834"Configuring Single Sign-On (SSO)" on page 838"How to Install the Delinea Browser Extension" on page 850"Configuring App Gateway" on page 852"Managing Application Sets" on page 830"Managing Application Access Requests" below"Removing an Application" on page 833

Managing Application Access Requests

In most cases, you give users access to applications by assigning them to one or more specific roles. You can also selectively define a "request and approval" workflow that gives specific users or members of specific roles the ability to approve or reject access requests for specific applications. You can configure the "request and approval" workflow for any of the individual web applications for which you want to manage access requests.

By defining a workflow, users can request access to an application and, if their request is approved, be added to a role with access privileges and see their new application available when they log on to the Admin Portal. A designated "approver" might be a specific user or any member of a specific role. If you configure a role as an approver, the first member to respond to the request is given the authority to approve or reject the request.

Configuring a Request and Approval Workflow

As a member of the sysadmin role or a role with the Role Management administrative right, you can configure roles for all other users. Initially, only the members of the sysadmin role have the ability to enable a "request and approval" workflow and can configure the workflow for selected applications, specify the users or roles with authority to approve access requests, and identify the role or roles to which users will be assigned if their request is approved.

At a high level, the steps involved in configuring a workflow are these:

- Create one or more roles that can enable a "request and approval" workflow.
- Create one or more roles that can approve access requests for the applications that have a "request and approval" workflow.
- Select an application and click **Workflow** to select the role into which requestor's who are approved will be placed.
- Select the user or role with authority to approve requests.

If the Requestor's Manager is the only approver in the approver list and the user has no manager, the request will be approved. If this is not desirable, verify that your users have a manager (refer to Adding Privileged Access Service users for more information) or add other users or roles to the approver list.

Creating Roles for Workflow Administration

The first few steps in configuring the “request and approval” workflow are optional and involve creating one or more roles for users who are allowed to define a “request and approval” workflow for applications and the roles that can approve access requests. These steps are optional because you can choose to only allow members of the sysadmin role to be the users permitted to configure a workflow and members of the sysadmin role can assign approval authority to individual users without creating any approval roles. In most cases, however, creating roles for different sets of users provides greater flexibility and helps to reduce the number of requests left pending an approval.

If you don’t create any intermediary roles with the appropriate administrative rights to enable a workflow, only members of the sysadmin role will be able to configure any “request and approval” workflow you might want to implement.

In most cases, if you are configuring a request and approval workflow for applications, you should create at least one role for users who are allowed to add, modify, or remove applications and who have permission to change which roles are assigned to a specific applications. If you don’t create a role with the Application Management and Role Management rights, only members of the sysadmin role can configure the “request and approval” workflow for applications.

To configure roles that can enable a workflow

1. Log in to Admin Portal.
2. Click **Access > Roles**.
3. Click **Add Role** or select an existing role to display the role details.

   If you are creating a new role, you must provide at least a unique name for the role.
4. Click **Members**, then click **Add**.
5. Type a search string to search for and select users and groups for this role.
6. Click **Administrative Rights**, then click **Add**.
7. Select the appropriate rights, then click **Add**.

   For example, if you are creating a role with permission to enable a workflow for access to applications, select Application Management and Role Management. You can select any additional rights you want included in this role, but you must select at least one of the required administrative rights.
8. Click **Save** to save the role.

Creating Roles for Approvers

You can assign approval authority to individual users. However, in most cases, creating “approver” roles for different sets of users provides greater flexibility and helps to reduce the number of requests left pending an approval. If you don’t create any intermediary roles with the appropriate administrative rights to approve access requests, only members of the sysadmin role will be able to approve access requests. You can follow the same steps described in "Creating Roles for Workflow Administration" above to create roles for approvers.

Keep in mind that if you are creating a role with permission to approve access requests for applications, you should include the Application Management and Role Management rights. You can select any additional rights you want included in this role.

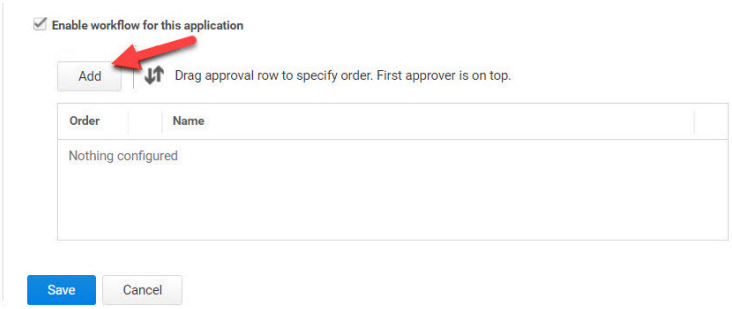
Configuring Workflow

As a member of the sysadmin role or a role with Application Management and Role Management administrative rights, you can configure a request and approval workflow for any application.

For more information, see "Managing Application Access Requests" on page 823.

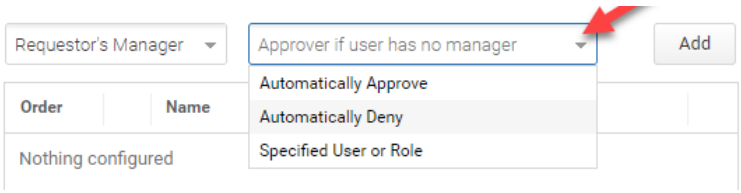
To configure workflow for applications

1. In Admin Portal, click the **Apps** tab, then select a specific application for which you want to configure a request and approval workflow.
2. Click **Workflow**, then select **Enable workflow for this application**.



3. Click **Add** (above) and select an **Approver Type** from the list (below).

Note: If you choose Requestor's Manager, you will also need to choose an option for how to handle the request if the user has no manager:



4. Click **Add** again to finish adding the approver type to the list.
5. If you want to have more than one approval before access to the app is granted, repeat the previous two steps.

   Adding steps can be repeated as many times as desired to reflect the required steps in your approval process.

Note: When multiple approval steps are added, approval is needed from all listed approvers before access is granted. A rejection at any level results in the request being rejected. If the requestor's manager is not known, the request proceeds to the next step as though it had been approved. The next approver in the list is notified that the manager was not known, and therefore there has not yet been any approval or rejection of the request.

Note: The first approver is the only one who can choose which role the user is added to.

Note: If the manager is the first approver and the requester does not have a manager, the requester will be placed into the first role in the role list if the app request is approved.

6. Click **Save**.

   After you have configured the workflow for an application, users can request access to the application through the Admin Portal.

Requesting Access to an Application

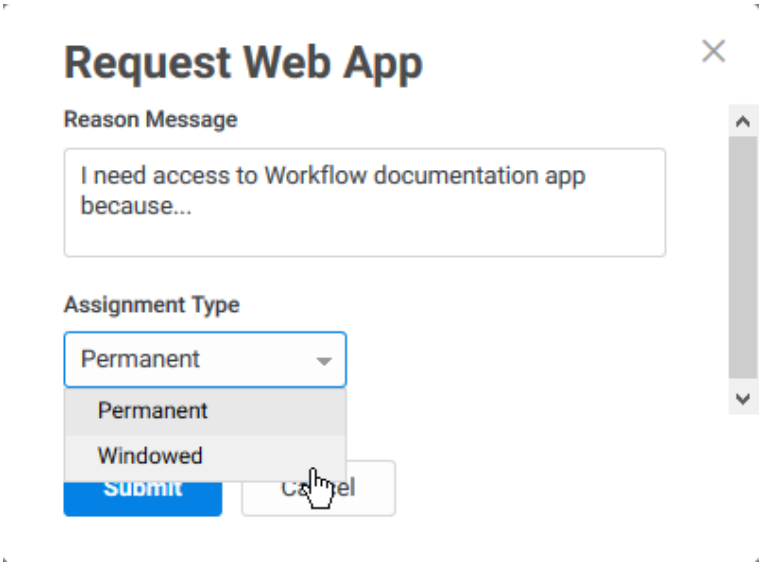
Any user who has an account in Privileged Access Service can request access to applications with workflow enabled. No special privileges are required to make requests or approve requests.

To request access to an application

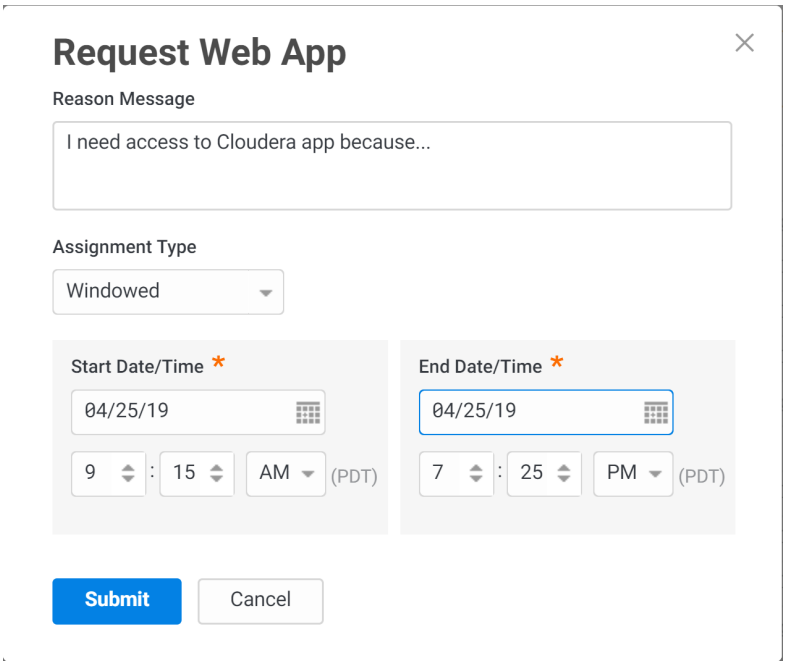
1. Log on to the Admin Portal.
2. Click **Apps > Add Web Apps**.
3. Type a search string to find the application of interest in the catalog, then right-click or select the check box next to the application.
4. Select **Request Launch** from the Actions menu.

   Only applications with workflow enabled display a Request Launch option.
5. Select either **Permanent** or **Windowed** in the Assignment Type drop-down menu.
   - Permanent - if the request is granted, the user will have access to the app for an indefinite time period, or until it is revoked by an administrator.
   - Windowed - if the request is granted, the user will have access to the app for the specified window, or until it

is revoked by an administrator.



6. (Optional) Select the start and end date and time if the request is for a windowed assignment type.



7. Type the business reason for requesting access to the application, then click **Submit** to continue.
8. Click **Close** to close the App Catalog.

   An email notification of your request is sent directly to the designated approver. You can click the Requests tab to see the status of your request. You will also receive an email notification when you request is approved or rejected. If your request was approved, the email will include a link to open the Admin Portal.

Viewing Request Status and History

You will only see the Requests tab if you have made a request or approved a request. After you have made or responded to at least one request, you can click the Requests tab to view the status of requests and the history of request activity.

The list of requests includes the following information:

- **Description** provides a brief summary of the request indicating the type of access or application requested.
- **Status** displays the current status of the request as Pending, Approved, Rejected, or Failed.

  You can review the request details to see the reason the request failed. For example, a request might fail if the email address for the approver or requester is invalid. A failed request might also indicate that the time allowed for taking the requested action has expired. For example, assume the request was for permission to use the root account to log on to a resource and the request was approved with a duration of 60 minutes. If the requester did not log on within 60 minutes of the request approval, the request status will display **Failed**.
- **Posted** displays the date and time of the most recent activity for each request.
- **Approver** displays the user or role designated for approving access requests if the approval is pending or the specific user who approved or rejected the request if the request has been resolved.
- **Requester** displays the user who submitted the request.
- **Latest Log Entry** displays the most recent information recorded for the request.

Viewing Request Details

You will only see the Requests tab if you have made a request or approved a request. After you have made or responded to at least one request, you can click the Requests tab to view the status of requests and the history of request activity.

If you are an approver, you can also go directly to Request Details by clicking the link in the email notifying you of the request.

Regardless of the entry point for viewing request details, the request information table displays details appropriate for the current state of the request. For example, you might see the following information:

- Posted displays the date and time of the most recent activity for each request.
- Description provides a brief summary of the request indicating the type of access or application requested.
- Requester displays the user who submitted the request.
- Requesters Reason displays the business reason provided by the user who submitted the request.
- Approver displays the user or role designated for approving access requests if the approval is pending or the specific user who approved or rejected the request if the request has been resolved.
- Status displays the current status of the request as Pending, Approved, Rejected, or Failed.

  Depending on the status of the request, you might see the reason the request was rejected or the reason why the request failed.

Responding to Application Access Requests

There are no special privileges required to respond to requests. Anyone with access to the Privileged Access Service can be designated as an approver.

If you have been designated as an approver for requests, you will receive an email notification when requests are received. You can click the **View Request** link in the email to view the request details. If you are authorized to approve the request and the request is still pending a response, the Request Details displays the options to Approve or Reject the request.

- Click **Approve** to approve the request and add the requester to the role selected for user access when the "request and approval" workflow was configured. If you click OK to continue with the approval, the request details are updated with the date and time the request was resolved and the approved status.
- Click **Reject** to reject the request and type the reason you are rejecting the request. If you click OK to continue with the rejection, the request details are updated with the reason the request was rejected, the date and time the request was resolved, and the rejected status.

After you respond to the request, the Requests tab is also updated with the latest activity and email is sent to the requester as notification of your response to the request.

To respond to application access requests

1. Access the request details by clicking **View Request** in the email notification or selecting **Access > Requests** and then clicking the request in the Admin Portal.

   The Approve Request window appears.

2. Click either **Approve** or **Reject** to respond to the request.

   Approve

   Reject

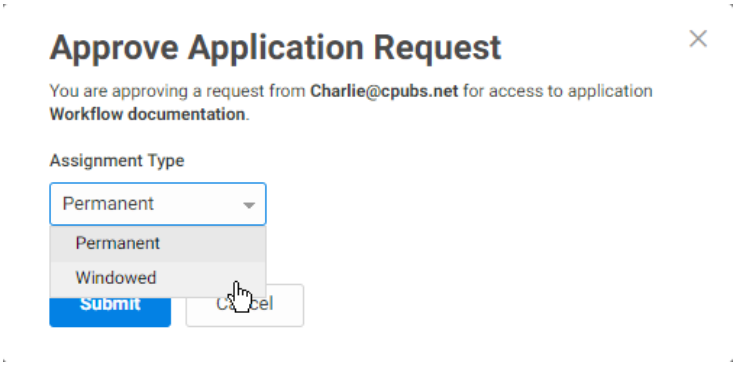
   a. Click **Approve** to approve the request and grant the requester the necessary permissions to the object.

      The Approve Request window appears.

   b. Select either **Permanent** or **Windowed** in the Assignment Type drop-down menu.

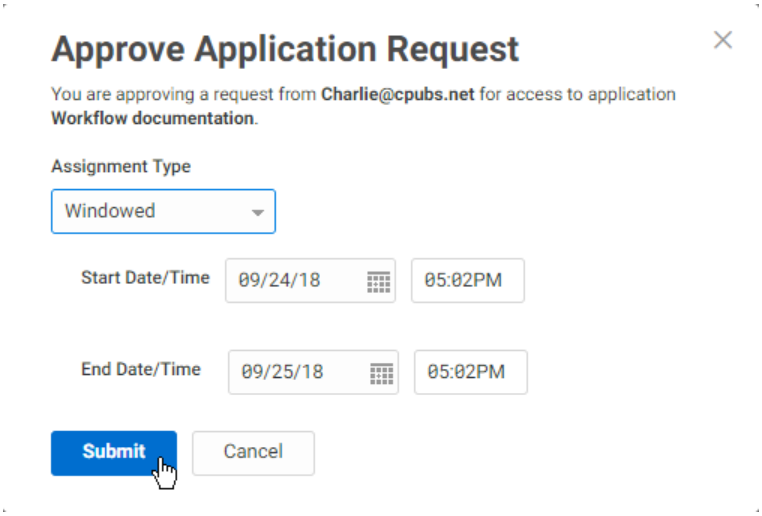
      i. Permanent - Grants the user access to the app for an indefinite time period, or until you revoke access.

      ii. Windowed - Grants the user access to the app for the specified window, or until you revoke access.



c. (Optional) Select the start and end date and time if the approval is for a windowed assignment type.

You can select a windowed approval regardless of the assignment type requested by the user. For example, you can approve access for a windowed time period if the user requested permanent access, or you can change the time window if the user requested windowed access.



d. Click **Submit**.

The request details are updated with the date and time the request was resolved and the approved status.

Click **Reject** to reject the request and type the reason you are rejecting the request. If you click **Submit** to continue with the rejection, the request details are updated with the reason the request was rejected, the date and time the request was resolved, and the rejected status.

Managing Application Sets

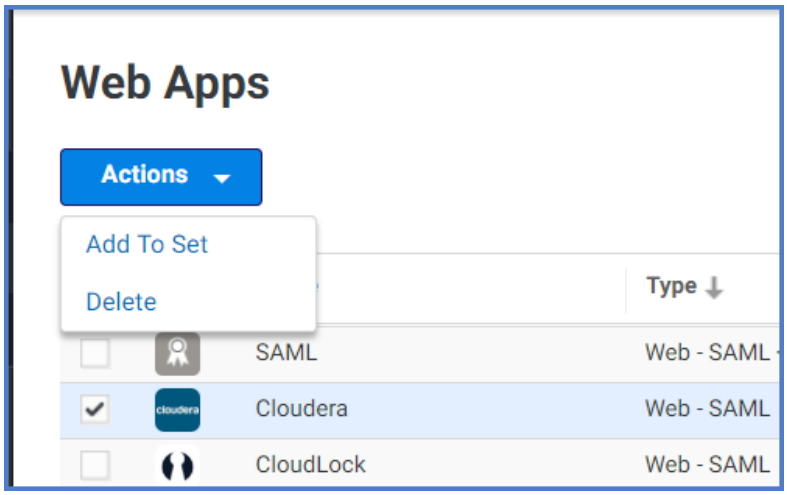
A set is a logical grouping of objects. An application set is a grouping of application objects. Organizing application objects into sets simplifies management and deployment of applications while offering more granular control. For example, you can use sets to deploy applications to not just roles, but individual users.

Applications have predefined sets that you can use as filters. For example, there are predefined sets for SAML Web applications, User Password Web applications, and more. You cannot modify the predefined sets.

In addition to the predefined sets, you can also create custom sets by manually adding and removing members or by defining queries. If you add a set, you can view and modify the set details and grant permissions to other users. You can manually add member objects to a set, or use a SQL query.

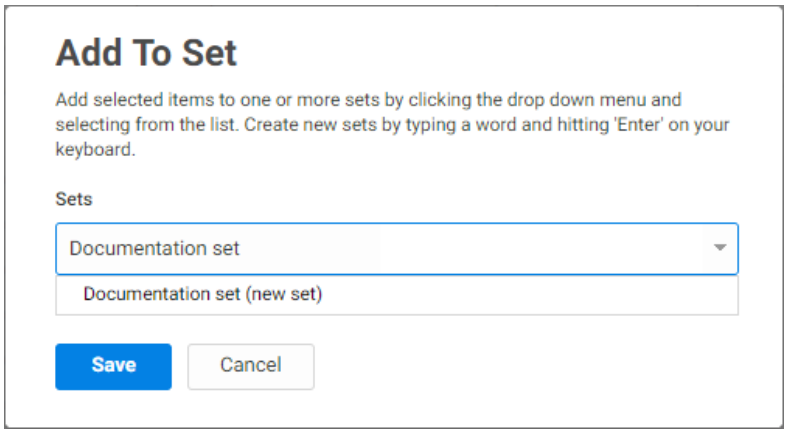
To add a manual application set

1. In the Admin Portal, click **Apps** to display the list of available applications.
2. Select the apps that you want to add to your new set, then click **Actions** > **Add to Set**.



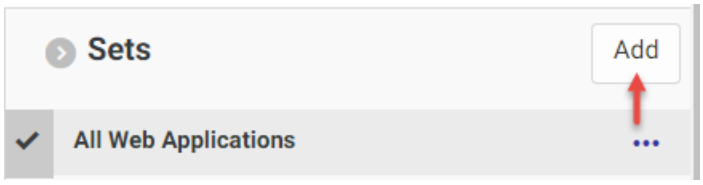
3. Type a name for the new set and an optional description, then click **Save**.

   If the set already exists, you will see autocomplete suggestions for the set. If it does not already exist, you will see (new set) in the field.



To add a dynamic application set

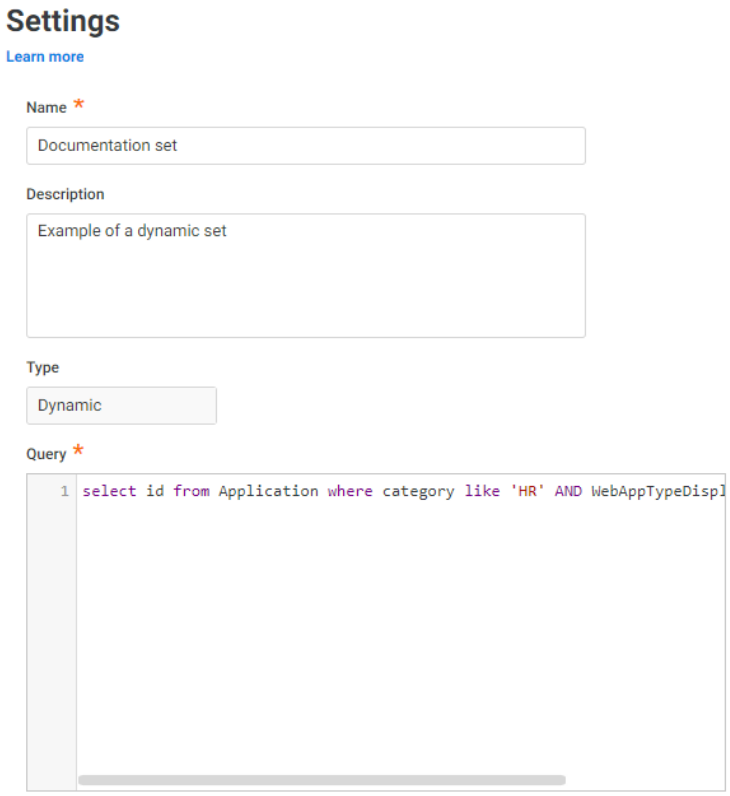
1. In the Admin Portal, click Apps to display the list of available applications.
2. In the Sets section, click **Add** to create a new set.



3. Type a name for the new set, an optional description, select **Dynamic** from the Type menu.
4. Type the SQL statement to execute to identify set members in the Query field.

For example, if you want to add a set for SAML-enabled HR applications, you could type a SQL statement like this:

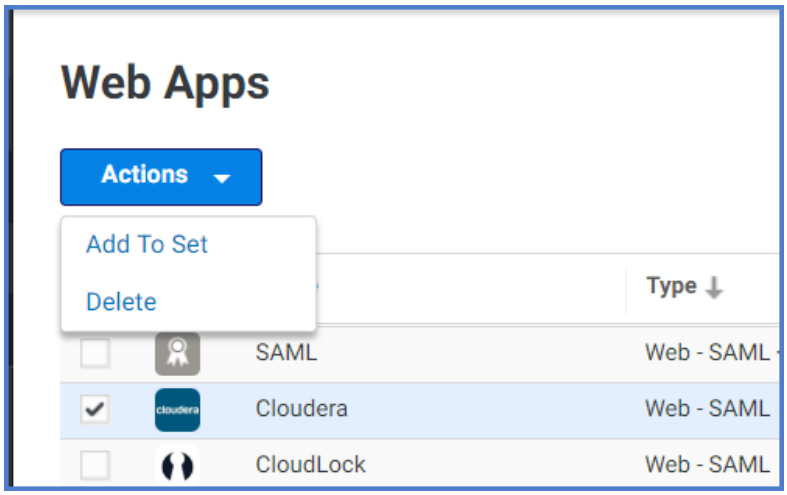
select id from Application where category like 'HR' AND WebAppTypeDisplayName like 'SAML'



5. Click **Save**.

To add applications to an existing manual set

1. In the Admin Portal, click **Apps** to display the list of available applications.
2. Select the apps that you want to add to your existing set, then click **Actions** > **Add to Set**.



3. Type the name for the set and an optional description, then click **Save**.

   If the set already exists, you will see autocomplete suggestions for the set. You can add an application to one or more sets.

To modify a set

1. In the Admin Portal, click **Apps** to display the list of available applications.
2. In the Sets section, right-click a set name, then click **Modify**.
3. Change the set name, set description, or both, as needed.
4. If the membership definition is dynamic, you can modify the set membership by editing the Query field.
5. Click **Save**.

To delete an application set

1. In the Admin Portal, click **Apps** to display the list of available applications.
2. In the Sets section, right-click a set name, then click **Delete**.
3. Click **Yes** at the confirmation prompt to delete the set.

   Deleting a set only deletes the grouping of applications; it does not delete the applications.

   For more information on desktop app sets, see "Adding Desktop App Sets" on page 932

Removing an Application

After deploying an application you can remove from the application list.

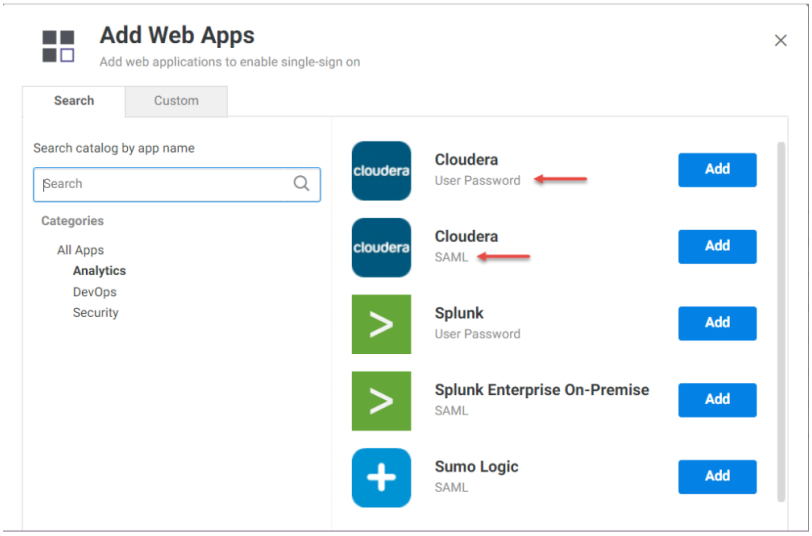
To remove an application:

1. In the Admin Portal, click **Apps > Web Apps**, to display the list of web applications in the applications list.
2. Select the box next to an application to display the Actions menu.
3. Click the Actions menu, then click **Delete**.
4. Click **Yes** to confirm that you want to proceed with deleting the application.

Adding web applications Select an application from the following list for more information on how to configure it in the Admin Portal.

Application Types

There are different types of applications that you can add and deploy to your users. The Delinea App Catalog lists the name and application type for each application.



- Web applications with user name and password authentication

  Some web applications are configured for user name and password authentication only.

- Web applications with SAML authentication

  Some web applications are configured to exchange authentication information between an identity provider (IdP) and a service provider (SP) to allow users that have already signed in to one app, to access their other apps without signing in again.

- Custom applications

  If your application is not listed in the catalog, you can use a custom template to provide access to that application. The types of custom applications are listed here with links to more information about each type:

  - **SAML applications**: allow you to create web applications that aren't in our catalog and that use SAML (Security Assertion Markup Language) for authentication. For more information, see "Custom SAML Applications" on page 961.
  - **User-Password** applications: allow you to create web applications that aren't in our catalog and if the application only supports user name and password authentication or if you don't want to configure the application for SAML SSO at this time. For more information, see "Adding User-password Applications" on page 975.
  - **OAuth2 Client** applications: OAuth 2.0 is an open-standard framework and specification for authorizing client applications to access online resources. Authorization works by requiring a client to obtain an access

token from a server that in turn grants the client access to specific protected resources. Use this template to set up an application that is making OAuth secured REST calls to Delinea.

- **OAuth2 Server** applications: Use the custom OAuth2 Server application for use with another web application's APIs. With the OAuth2 Server application, you can set custom claims in the resulting access token. Use this template if you need to have OAuth tokens generated for consumption by an application.

- Desktop Applications

  Provide the ability to configure and launch desktop applications that reside on a remote application host system. You can add desktop applications such as SQL Server Management Studio, TOAD for Oracle, and VMware vSphere Client, as well as custom applications that aren't in our Delinea Desktop App Catalog, using the generic application template. For more information, see "Adding Web Applications Using the Admin Portal" on the next page.

SAML SSO options

Web applications that support SAML can use the Privileged Access Service to securely authenticate users. The Service Provider (SP) is the web application that users request to log in to via the Privileged Access Service (also called the Identity Provider, IdP).

A signing certificate (X.509), establishes a trust relationship between the SP and the IdP. The IdP uses the X.509 certificate to sign the XML and the SP checks the signature that it receives with a certificate it has on file. With that trust relationship in place, the SP consumes the assertion passed to it from the IdP and allows users to authenticate without requiring additional credentials.

Web applications that support SAML authentication offer the following authentication methods:

- IdP-initiated only

  IdP sends SAML Response to the SP.

- SP-initiated only

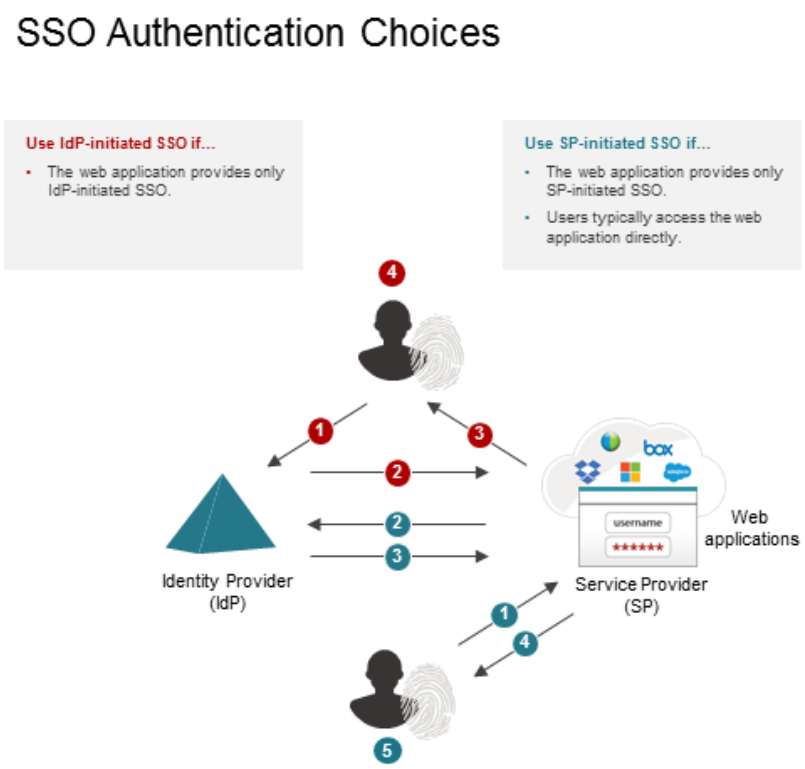
  The SP sends the SAML Request to the IdP; IdP sends SAML Response to the SP.

- IdP-initiated and SP-initiated

  
  The response is sent to the Assertion Consumer Service (ACS) URL configured during application setup.

In most cases, if you use IdP-initiated SSO, your users can still access the application directly using their user name and password. If you use SP-initiated SSO, your users are redirected to log in directly to the web application. Some applications prevent user name and password logins.

The following diagram illustrates the main differences between IdP-initiated and SP-initiated SSO.



IdP-initiated SSO	SP-initiated SSO
User logs on to the Admin Portal (IdP); IdP authenticates the user. IdP generates a security token and redirects the user to the web application (SP site). SP grants access to the user. User is logged on to the web application.	User accesses the web application (SP site). SP redirects the user to the IdP. IdP authenticates the user, generates a security token and redirects back to the web application (SP site). SP grants access to the user. User is logged on to the web application.

Adding Web Applications Using the Admin Portal

You can add web applications and then configure and deploy them to users in one session. Alternatively, you can add the applications to your Admin Portal Apps page and then configure and deploy them at a later time. The Status column shows the application status–see "Viewing and Sorting Applications in the Apps Page" on page 838. You need to configure an application and deploy it to a role before users can use single-sign-on to access it.

You can add web applications using the following methods:

- From the Privileged Access Service App Catalog
- Using a custom application.

Adding Web Applications From the Privileged Access Service App Catalog

The Privileged Access Service App Catalog contains an ever-expanding list of web applications ready for assignment to users. If the web application is not in the catalog, you can open a custom application in the catalog and fill in the details.

To add a web application from the App Catalog

1. Log in to Admin Portal.
2. Click **Apps** > **Add Web Apps**.

   The Add Web Apps window opens.
3. Use the information on the Search tab to select the application or applications.

   See "Using a Custom Application" below to add an application using one of the custom applications.
4. Select the application or applications.

   Click the **Add** button to select one or more applications.

   You can continue to select categories and add more applications. You can add up to 30 applications in one session.

   If you change your mind, click Remove.
5. Click **Close**.

   If you added just one application, Admin Portal opens the configuration window for that application. If you added more than one application, Admin Portal opens the Apps page. You click the application name to configure it. Click **Help for this application** for the configuration instructions.

Using a Custom Application

The Privileged Access Service App Catalog includes custom applications that you can add and fill in to add applications. Click the Custom tab to display the list of custom applications. Click the information icon associated with each template for a description.

To add an application from a template

1. Open Admin Portal and click the **Apps** tab.
2. Click **Add Web Apps**.

   This opens the Add Web Apps window.
3. Click the **Custom** tab.
4. Click **Add** for the template you want and click **Yes** in the confirmation window.
5. Click **Close**.

   This closes the Add Web Apps window and opens the configuration window.
6. Click **Help for this application** for the configuration instructions.

Viewing and Sorting Applications in the Apps Page

The Apps page lists all of the applications you have added to the Privileged Access Service. You can use the column headers to sort applications and quickly find the one you are looking for.

> Your role must have the Privileged Access Service Applications Management administrative right to view, add, and modify applications.

Application Status

An application can have one of the following statuses:

- **Not Configured:** All required fields have not been defined.
- **Ready to Deploy**: (web applications) All required fields have not been defined and you have not assigned the user access.
- **Deployed**: All the required fields have been defined and user access has been assigned. Users assigned to the roles with this application deployed can now access the application from their Privileged Access Service Admin Portal or devices.

Application Types

You can also filter the applications displayed by type. Use the Search drop-down menu to select the type. The application types are defined as follows:

Application type	Description
SAML Web	Web applications that use SAML for authentication
SSO Web	Web applications that use either SAML, or vendor specific federated authentication
User Password Web	Web applications that use user name and password for authentication
Web	All Web applications.
Other Type	Web applications that use OAuth tokens.

Configuring Single Sign-On (SSO)

If the web application uses SAML for single sign-on purposes, there are additional configuration options. For more information, see the instructions for the application you want to configure. To access application-specific instructions, click the **Application Configuration Help** link in the application setup page in Delinea Admin Portal, or search Delinea help for the application you want to configure.

Application-specific settings are configured in the application configuration pages available once you add an application from the App Catalog. Some of the pages are required in order to deploy the application and others are optional or are not available.

See the following for additional information on each configuration page:

Configuration page	Additional Information
Trust	"Configure Application-specific Settings" below"Choose a Certificate File" on page 842
Settings	"Changing the App Name, Description, or Logo" on page 844"Specifying the Application ID" on page 844
User Access	"Deploying Applications" below
Policy	"Specifying Additional Authentication Control" on page 845
Account Mapping	"Map User Accounts" on the next page
SAML Response	"Editing the Assertion Script" on page 849
App Gateway	"Accessing Applications Outside the Network" on page 849
Changelog	"Viewing a Log of Recent Changes" on page 850
Workflow	"Viewing a Log of Recent Changes" on page 850

Configure Application-specific Settings

On the Trust page, you configure the application-specific settings in order to connect the application to the Privileged Access Service and enable SSO. Most applications require you to configure settings specific to that application, however the specific parameters may vary for each type of application (SAML, password). For information about choosing a security certificate file for an application, see "Choose a Certificate File" on page 842.

For detailed configuration information for web applications, see "Adding Web Applications Using the Admin Portal" on page 836.

Deploying Applications

You must assign users permissions for an application before that application is available to users for single sign-on. You can use one of the following methods to assign user permissions:

- Assign permissions to user(s), group(s), and role(s) at the application level.
- Assign member permissions to user(s), group(s), and role(s) for a set of applications.

  Refer to "Managing Application Sets" on page 830 for more information.

You must be a member of the sysadmin role or a role that has the Application Management permission to configure and deploy applications.

To assign permissions to for an application

Set permissions on the application.

1. On the Permissions page, click **Add**.

   The Select User, Group, or Role window appears.
2. Select the user(s), group(s), or role(s) that you want to give permissions to, then click **Add**.

   The added object appears on the Permissions page with View, Run, and Automatically Deploy permissions selected by default.
3. Select the desired permissions, then click **Save**.

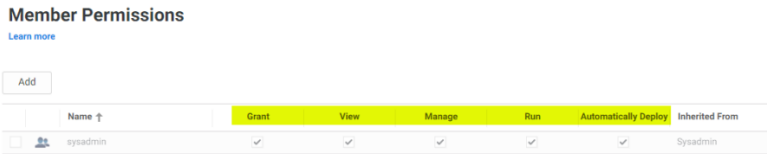
Add the application to a set.

1. Add the application to an appropriate set.

   You can either create a new set or add the application to an existing set. Refer to "Managing Application Sets" on page 830 for more information about creating and modifying application sets.
2. In the Sets section, right-click a set name, then click **Modify**.
3. On the Member Permissions page, click **Add**.

   The Select User, Group, or Role window appears.
4. Select the user(s), group(s), or role(s) that you want to give permissions to, then click **Add**.

   The added object appears on the Permissions page with View, Run, and Automatically Deploy permissions selected by default.
5. Select the desired permissions, then click **Save**.

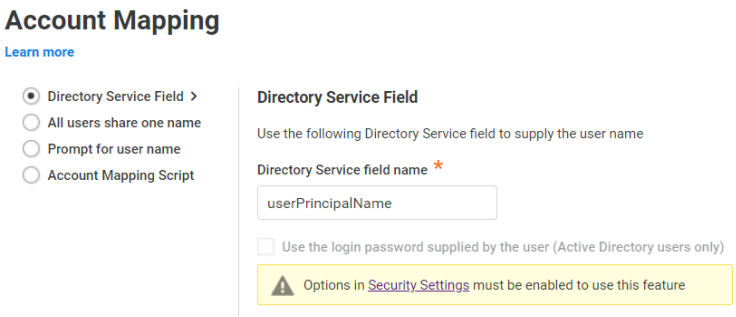


Map User Accounts

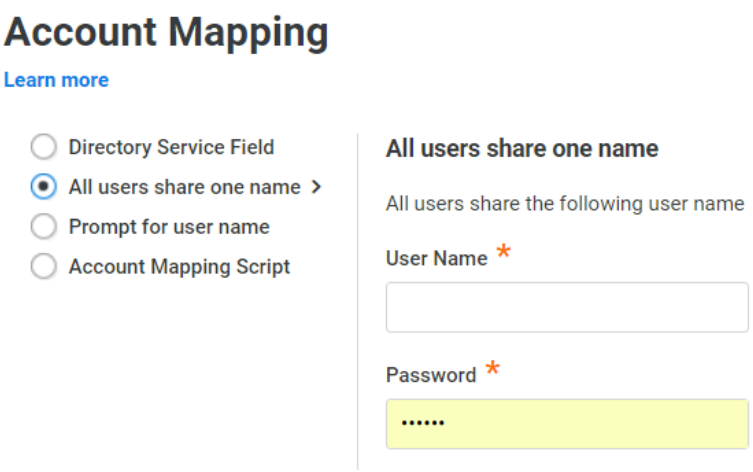
On the **Account Mapping** page, configure how the login information is mapped to the application's user accounts. Depending on the type of application that you select, the options that you see might be different than those shown here.

Depending on your application, available options might vary slightly.

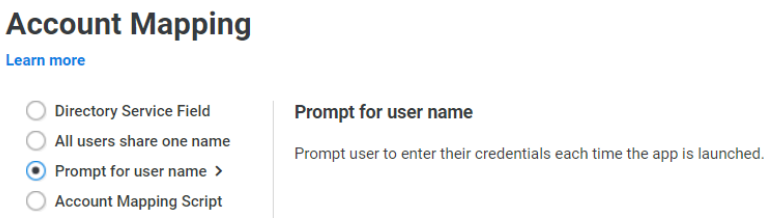
- **Directory Service Field**: Use this option if the user accounts are based on user attributes. For example, specify an Active Directory field such as *mail* or *userPrincipalName* or a similar field from the Delinea Directory.



- **All users share one name**: Use this option if you want to share access to an account but not share the user name and password. For example, some people share an application developer account.



- **Prompt for user name:** Use this option if you want users to supply their own user name and password. This option only applies to user password application types. The first time that users launch the application, they enter their login credentials for that application. The Delinea Directory stores the user name and password so that the next time the user launches the application, the Delinea Directory logs in the user automatically.

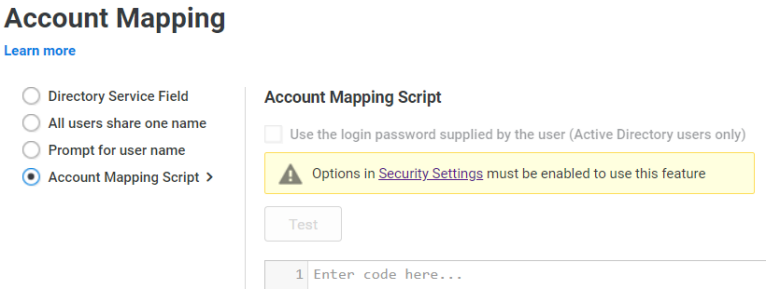


- **Account Mapping Script**: You can customize the user account mapping here by supplying a custom JavaScript. For example, you could use the following line as a script:

  LoginUser.Username = LoginUser.Get('mail')+'.ad';

  The script sets the login user name to the user's mail attribute value in Active Directory and adds '.ad' at the end. For example, if the user's mail attribute value is Adele.Darwin@acme.com then the account mapping script sets

LoginUser.Username to Adele.Darwin@acme.com.ad. For more information about writing a script to map user accounts, see the "SAML Application Scripting" on page 1001.



Choose a Certificate File

On the **Trust** page you can select a certificate provided by the Privileged Access Service or you can upload your own certificate to establish secure SSO authentication between the Privileged Access Service and the web application. Most applications can be configured using the default tenant signing certificate, but if you want to use your own certificate, you can choose **-Upload New Signing Certificate-** from the Security Certificate drop down menu.

Be sure to use a matching certificate both in the Admin Portal and in the application itself.

In most cases the SignatureMethod Algorithm in the certificate matches the DigestMethod Algorithm in the SAML assertion; however, some applications might require a different DigestMethod Algorithm. In those cases, you can use the setDigestMethodAlgorithm method in the SAML assertion script to manually set the DigestMethodAlgorithm.

setDigestMethodAlgorithm specifies the digest method algorithm to use in the SAML response. Possible values are:

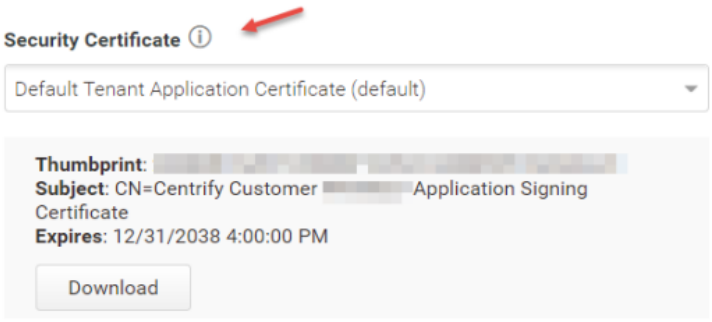
- sha1
- sha256
- sha384
- sha512

The default value is the same as the SignatureMethod algorithm for the signing certificate selected for the app. For example, setDigestMethodAlgorithm('sha256').

To select a signing certificate for an application

1. Select an application in the Admin Portal , then click **Trust**.
2. In the Identity Provider Configuration area, expand the certificate section and then select one of the following options:

> Depending on the application, the certificate section might say Security Certificate, X.509 Certificate, Signing Certificate, etc.



- Default Tenant Application Certificate (default)

  Select this option to use the Privileged Access Service standard certificate. This is the default setting.

  Click **Download** to save the certificate so you can use it during the application configuration process.

  If you replace the certificate, be sure to update the application with the new certificate information.

  > Any certificates uploaded to the Privileged Access Service tenant from the **Settings > Authentication > Platform > Signing Certificates** are also shown in the drop down list. You can choose from any of those certificates as well. For more information on uploading certificates to be part of the standard set of available certificates, see "How to Manage Tenant Signing Certificates" on page 300.

- -Upload New Signing Certificate-

  Select this option to upload your organization's own certificate. To use your own certificate, you must enter a name and a password (if the file requires a password) and then click **Browse** to upload an archive file (.p12 or .pfx extension) that contains the certificate along with its private key. Once uploaded, this certificate will also be listed in the list of certificates in **Settings > Authentication > Platform > Signing Certificates** and therefore available to all application deployments in the future.

  Upload the certificate from your local storage prior to downloading any IdP metadata. If the IdP metadata is available from a URL, be sure to upload the certificate prior to providing the URL to your service provider.

3. Click **Save**.

Integrating with Cloud Access Security Brokers (CASBs)

Delinea partners with CASBs to provide the first critical steps in enabling secure SaaS applications. By driving the authentication process through Delinea, CASBs utilize the necessary information about users, their devices, and their location to manage access to and monitor user activity within apps.

Delinea Admin Portal integrates with CASBs by passing the SAML assertion for a supported application to a CASB proxy, instead of directly to the service provider. The CASB then passes the SAML assertion on to the service provider.

Application support for CASB integration depends on your CASB provider. Contact your CASB provider for more information.

To direct a SAML assertion to a proxy

1. Open the Advanced page for the application that you want the SAML assertion to point to a CASB proxy.

   For more information, refer to the application configuration help specific to the that application.

2. Add the following line to the end of the advanced script. Refer to "Custom SAML Applications" on page 961 for more information about writing advanced scripts.

   setHttpDestination('CASBProxyURI');

   CASBProxyURI is the proxy URI provided by the CASB. It must be an absolute URI.

   Note: This line must be at the end of the script to prevent conflicts with other elements of the script.

3. Click **Save**.

Optional Configuration Settings

The following settings offer additional functionality and control, but do not need to be completed in order to deploy an application.

Specifying the Application ID

On the Settings page, you can configure an Application ID for mobile applications that use the Delinea mobile SDK. The Privileged Access Service uses the Application ID to provide single sign-on to mobile applications. Note the following:

- The Application ID has to be the same as the text string that is specified as the target in the code of the mobile application written using the mobile SDK. If you change the name of the web application that corresponds to the mobile application, you need to enter the original application name in the Application ID field.
- There can only be one SAML application deployed with the name used by the mobile application.

  The Application ID is case-sensitive and can be any combination of letters, numbers, spaces, and special characters up to 256 characters.

Changing the App Name, Description, or Logo

On the Settings page, you have the option to modify settings to change how and where applications are displayed in the Admin Portal Apps page.

To optionally change the app name, description, or logo

1. Click **Settings** in the Admin Portal.
2. Enter the new name in the **Application Name** field to change how the application name is displayed in the Admin Portal Apps page.

   Note: For some applications, the name cannot be modified.

3. Enter the new description in the **Application Description** field to change the default application description displayed in the Admin Portal Apps page.
4. Click **Select Logo** and upload a new logo file and change the default logo for the application displayed in the Admin Portal Apps page.
5. Click **Save**.

Specifying Additional Authentication Control

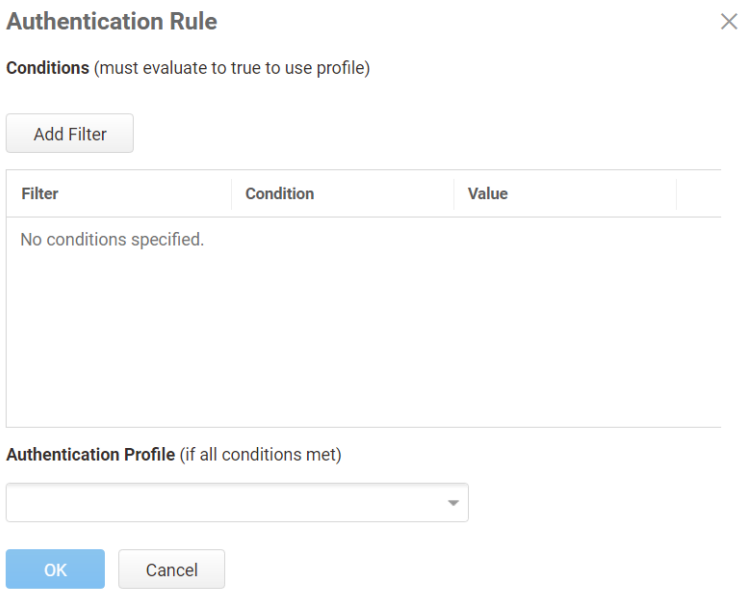
On the **Policy** page, can specify additional authentication controls for an application by defining rules and the order in which the rules are applied.

You can also include JavaScript to identify specific circumstances (log ins from outside corporate IP ranges) when you want to block an application or you want to require additional authentication methods. For details, see "Application Access Policies with JavaScript" on page 987.

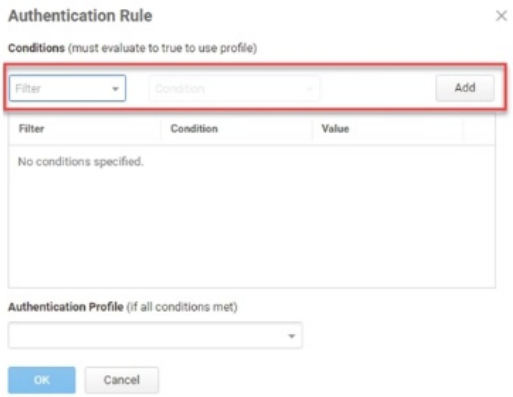
To define a rule that specifies additional authentication control

1. Click **Policy** in Admin Portal.
2. (Optional) Click **Add Rule** to specify conditional access.

   The Authentication Rule window displays.



3. Click **Add Filter** on the Authentication Rule window.
4. Define the filter and condition using the drop-down menus.



For example, you can create a rule that requires a specific authentication method when users access Privileged Access Service from an IP address that is outside of your corporate IP range. Available filters vary depending on the object they are applied to and features enabled on your tenant. Supported filters are:

Filter	Description
IP Address	The authentication factor is the computer's IP address when the user logs in. This option requires that you have configured the IP address range in Settings, Network, Corporate IP Range.
Identity Cookie	The authentication factor is the cookie that is embedded in the current browser by Privileged Access Service after the user has successfully logged in.
Day of Week	The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.
Date	The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.
Date Range	The authentication factor is a specific date range.
Time Range	The authentication factor is a specific time range in hours and minutes.
Device OS	The authentication factor is the device operating system.
Browser	The authentication factor is the browser used for opening the Privileged Access Service portal.

Filter	Description
Country	The authentication factor is the country based on the IP address of the user computer.
Certificate Authentication	The certificate is used for authentication.
For the Day/Date/Time related conditions, you can choose between the user's local time and Universal Time Coordinated (UTC) time.	

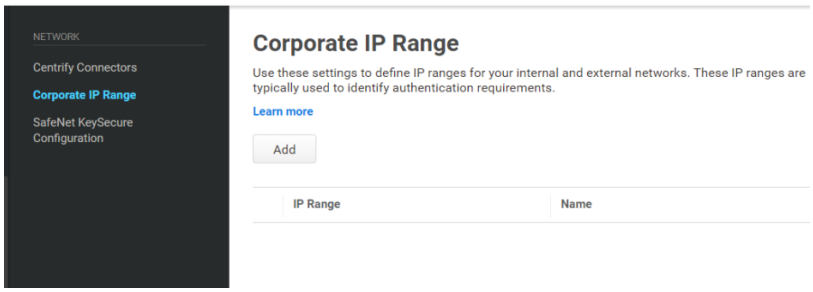
5. Click the **Add** button associated with the filter and condition.
6. Select the profile you want applied if all filters/conditions are met in the **Authentication Profile** drop-down.

   The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the **Add New Profile** option. See "Creating Authentication Profiles" on page 284.
7. Click **OK**.
8. (Optional) In the **Default Profile (used if no conditions matched)** drop-down, you can select a default profile to be applied if a user does not match any of the configured conditions.

   Note: If you have no authentication rules configured and you select **Not Allowed** in the **Default Profile** drop-down, users will not be able to log in to the service.
9. (Optional) If you have more than one authentication rule, you can drag and drop the rules to a new position in the list to control the order they are applied.
10. Click **Save**.

To specify a corporate IP range

Click **Settings > Network > Corporate IP Range**, then click **Add** and enter one or more IP addresses or ranges.

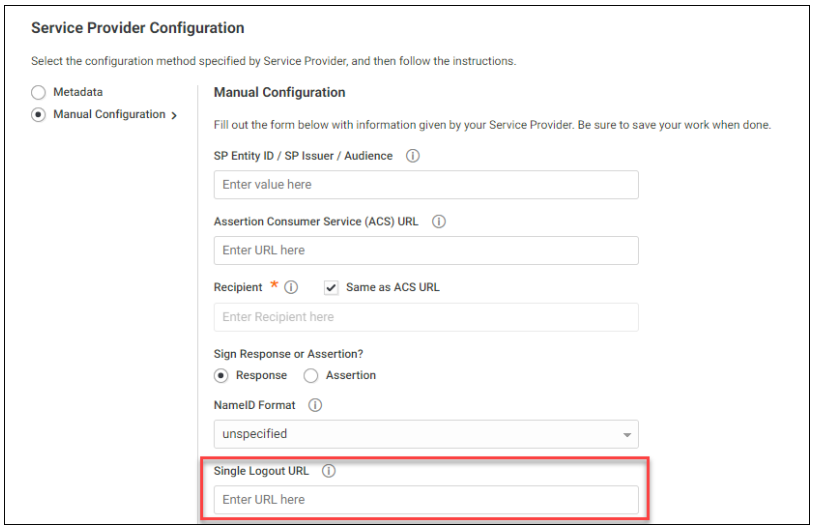


Note: If you left the Apps section of Admin Portal to specify additional authentication control, you will need to return to the Apps section before continuing by clicking **Apps** at the top of the page in Admin Portal.

Configuring Single Logout

If your service provider supports single logout ("SLO"), you can configure the application so that when your users log out of the application, they are also logged out of the Delinea Admin Portal.

To configure SLO, enter the Single Logout URL provided by your service provider on the Trust page under **Service Provider Configuration** > **Manual Configuration** > **Single Logout URL**.



Note: If you are configuring single logout in the B2B app, you must include the nameID attribute in the SAML response to facilitate SAML SP and IdP logout. Without the nameID attribute, only the Delinea tenant will be logged out, not the IdP.

With SLO configured, signing out of the application sends a logout request to the Privileged Access Service at the Identity Provider Logout URL (an automatically generated URL). The Privileged Access Service validates the request and returns a logout response to the service provider at the Single Logout URL.

Configure the SAML Attributes

On the SAML Response page, use the Attributes section to configure SAML attributes that should be included in the SAML response for this application.

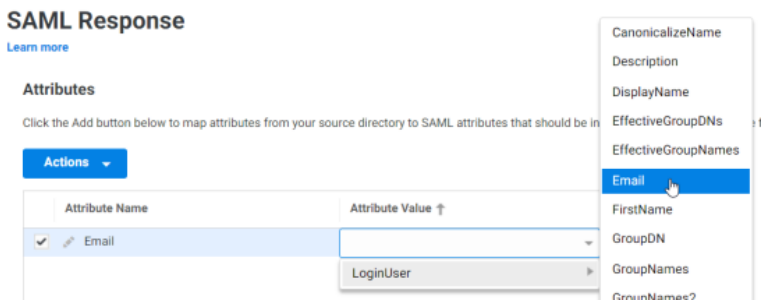
To add an attribute

1. Click **Add**.
2. In the Attribute Name field, enter the attribute name as required by the Service Provider.

   For example: Email
3. In the Attribute Value field, click the drop-down menu and the applicable value for the attribute name.

   For example: LoginUser.

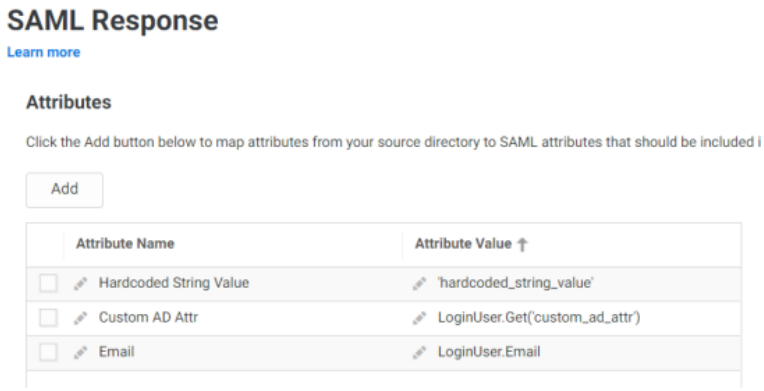
   Click the drop-down menu again and select **Email** from the popup menu to obtain LoginUser.Email.



4. Repeat the previous steps as necessary to add additional attributes.
5. If the drop-down menu items do not list the attribute that you want, click the input field and enter the value manually.

   For example, if you want an Active Directory attribute such as custom_ad_attr, enter LoginUser.Get('custom_ad_attr').

   If you want a hardcoded string value, enter the value enclosed in single quotes such as 'hardcoded_string_value'.



6. Click **Save**.

> **Note:** The attributes that you configure in the Attributes section are separate from those that you configure in the Custom Logic section. Both attribute entries appear in the SAML Response.

Editing the Assertion Script

If you use either the Advanced page or the SAML Response page, you have the option to edit the script that generates the assertion, if needed. In most cases, you don't need to edit this script. For more information on editing the SAML Response, see "SAML Application Scripting" on page 1001. For details on editing the assertion for user password applications, see "User-Password Application Scripting" on page 1024.

Accessing Applications Outside the Network

On the **App Gateway** page in Admin Portal, you have the option to configure secure access to on-premise applications outside of your corporate network without using a VPN connection. See "Configuring an Application to Use the App Gateway" on page 855for detailed configuration instructions.

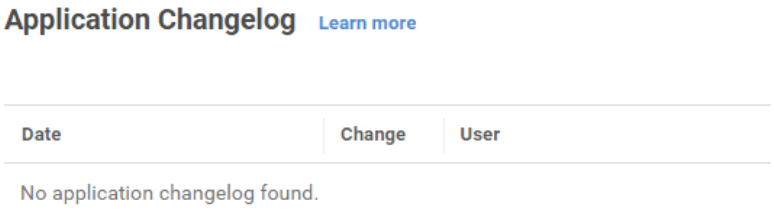
Setting up a Request and Approval Workflow

On the **Workflow** page you have the option to set up a request and approval workflow for an application.

See "Managing Application Access Requests" on page 823 for more information.

Viewing a Log of Recent Changes

On the **Changelog** page, you have the option to see recent changes that have been made to the application settings, by date, user, and the type of change that was made.

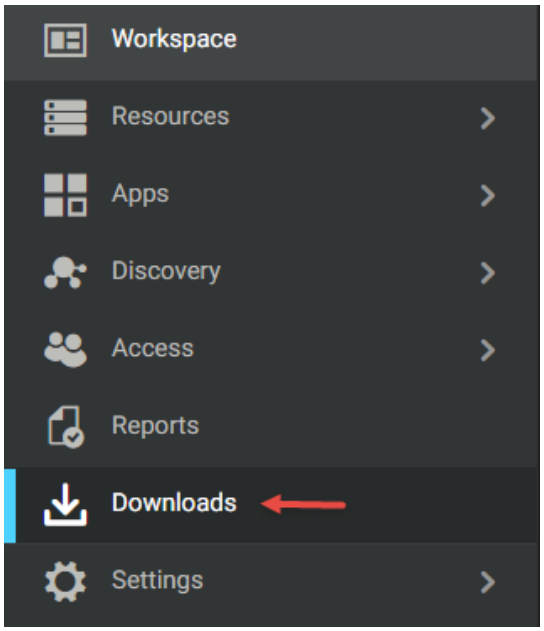


How to Install the Delinea Browser Extension

This scenario is intended to guide system administrators through the procedures for installing the Delinea Browser Extension. Some web applications require installation of the Delinea Browser Extension to provide single sign-on. Without the browser extension, users will not be able to open these applications. You only need to install the browser extension one time per browser type.

The installation link and the browser extension files for Chrome, Firefox, Safari, and Internet Explorer are available in the Downloads item in the account name drop down menu in Admin Portal.

> You can only update the browser extension; reverting to previous versions is not supported.



Installing the Delinea Browser Extension for IE on Remote Windows computers

You can automate the installation of the Delinea Browser Extension(Internet Explorer version) onto remote Windows computers using a silent installation or using a Windows Group Policy Object (GPO).

Computers must have Microsoft Installer 3.1 or later to install the Delinea Browser Extension.

To deploy the browser extension on remote Windows computers using a “silent” unattended installation or using a GPO, you need to specify the appropriate command line options and Microsoft Windows Installer (MSI) file. You can also use a software distribution product, such as Microsoft System Center Configuration Manager (SCCM), to deploy software packages.

An automated installation may fail if remote computers do not have the appropriate configuration. If you are installing silently or from a GPO, verify that the remote Windows computers meet the requirements described in System requirements and supported browsers.

To install the Delinea Browser Extension for Windows silently:

1. Open a Command Prompt window or prepare a software distribution package for deployment on remote computers.

   For information on preparing to deploy software on remote computers, see the documentation for the specific software distribution product you are using. For example, if you are using Microsoft System Center Configuration Manager (SCCM), see the Configuration Manager documentation.

2. Run the installer for the browser extension package for a 32-bit or 64-bit architecture.

   Note: If the system has a 64-bit operating system, use the 64-bit package, CentrifyIEExtensionSetup (x64).msi. CentrifyIEExtensionSetup(x64).msi includes the binary for both 32-bit and 64-bit versions of Internet Explorer.

   For example, on 32-bit operating systems, run the following command:

```
msiexec /qn /i "CentrifyIEExtensionSetup(x86).msi"
```

On 64-bit operating systems, run the following command:

```
msiexec /qn /i "CentrifyIEExtensionSetup(x64).msi"
```

To install the Delinea Browser Extension from a Group Policy Object:

1. Copy the CentrifyIEExtensionSetup(x64).msi files to a shared folder on the domain controller or another location accessible from the domain controller.

   If you are installing on a 32-bit architecture, the installer file name is CentrifyIEExtensionSetup(x86).msi. When you select a folder for the installer file, you might want to right-click and select **Share with > Specific people** to verify that the folder is shared with Everyone or with appropriate users and groups.
2. On the domain controller, click **Start > Administrative Tools > Group Policy Management**.
3. Select the domain or organizational unit that has the Windows computers where you want to deploy the browser extension, right-click, then select **Create a GPO in this domain, and Link it here**.

   For example, you might have an organizational unit specifically for Privileged Access Service-managed Windows computers. You can create a Group Policy Object and link it to that specific organizational unit.
4. Type a name for the new Group Policy Object, for example, Privileged Access Service Browser Extension Deployment, then click **OK**.
5. Right-click the new Group Policy Object, then click **Edit**.
6. Expand **Computer Configuration** > **Policies** > **Software Settings**.
7. Select Software installation, right-click, then select **New** > **Package**.
8. Navigate to the folder you selected, select the .msi installation file, then click **Open**.
9. Select **Published**, then click **OK**.
10. Close the Group Policy Management Editor, right-click the Privileged Access Service Browser Extension and verify Link Enabled is selected.

By default, when computers in the selected domain or organizational unit receive the next group policy update or are restarted, the browser extension will be deployed and the computer will be automatically rebooted to complete the browser extension deployment. If you want to test deploy, you can open a Command Prompt window to log on to a Windows client as a domain administrator and force group policies to be updated immediately by running the following command:

gpupdate /force

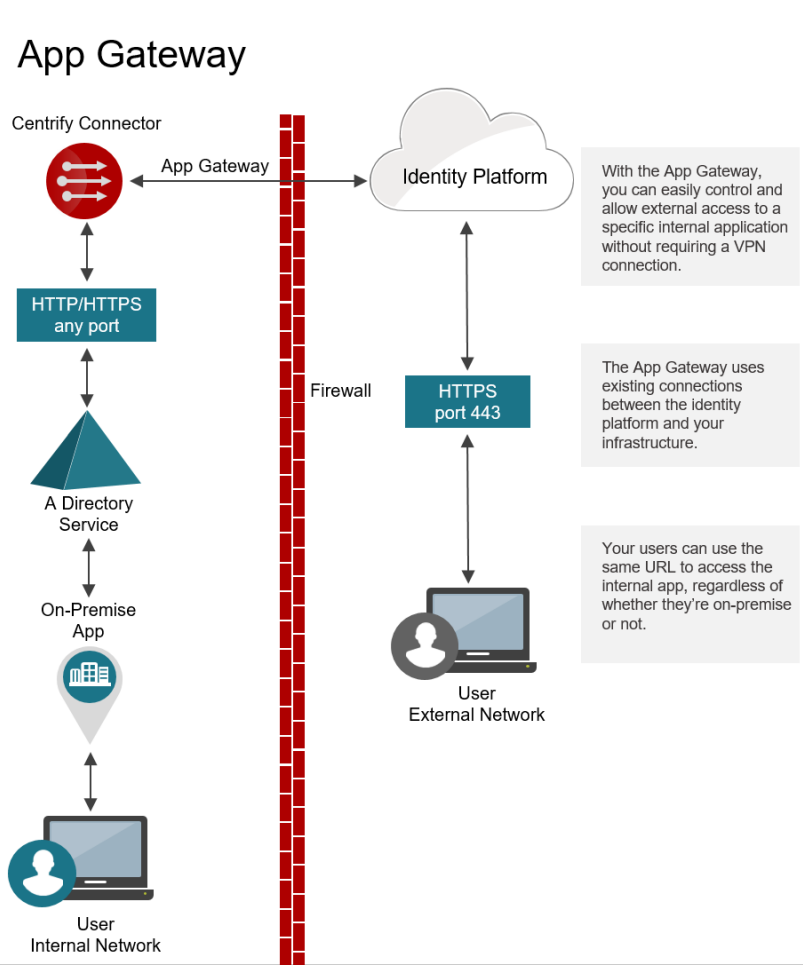
For more information about how to configure and use Group Policy Objects, see the documentation on the Microsoft Windows website.

Configuring App Gateway

You can configure on-premise applications so that your users can securely access them outside of your corporate network. Currently, you can require a VPN connection for application access by applying an access policy to the application. VPN connections are relatively straightforward to set up for your entire network, but configuring them to allow or not allow specific applications can be a lot of work. With App Gateway, you can now configure applications for off-site access without requiring a VPN connection.

When users launch an application through a VPN connection, the connection travels an additional pathway. With most VPN connections, the user can access most applications and servers on the corporate network, even if they don't need to do so. If your users need to visit other corporate networks, such as when your sales or other teams visit your customers, your users may not be able to easily launch a VPN connection. And, using VPN connections to access applications off-site can increase the traffic through your VPN tunnel.

For your users, the experience is simple—they enter the application URL and can directly launch the application. In most cases, you'll want to configure the application so that your users can use the same URL to access the application whether they're on the internal network or outside the corporate network.



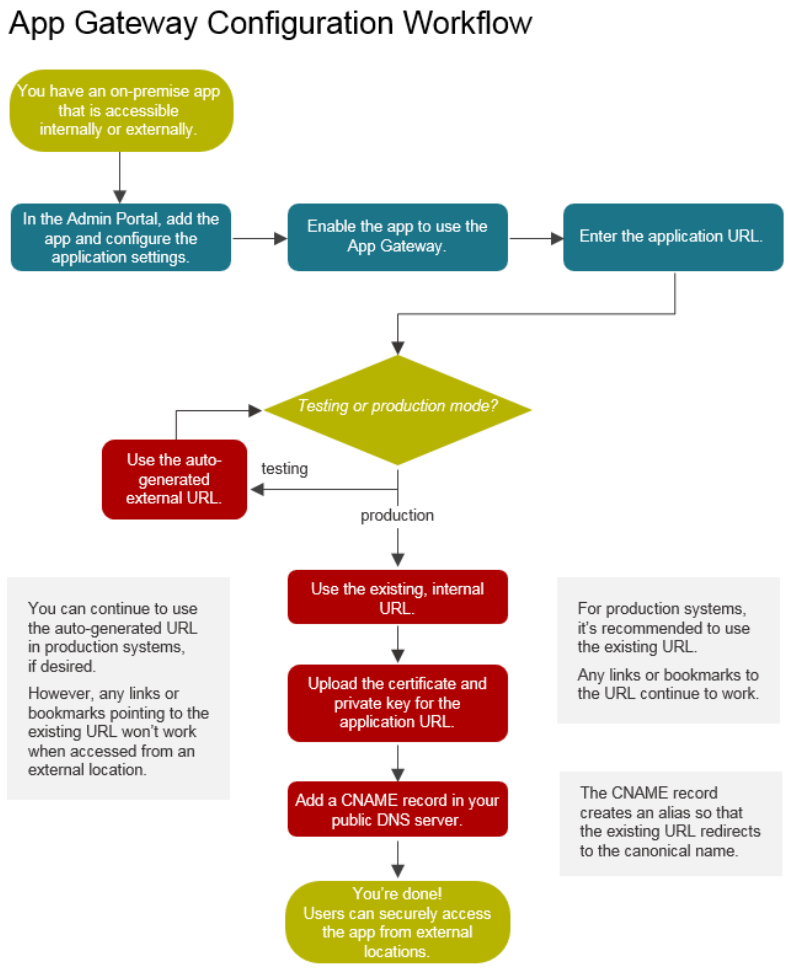
For applications that use the App Gateway, the connection from the user travels the same network pathways that you already have: the Privileged Access Service connects to the Delinea Connector through the firewall, the Delinea Connector connects to your on-premise directory service, and your on-premise application uses your directory service for authentication and authorization.

For more information on configuring App Gateway, see the following topics:

- "App Gateway Configuration Workflow" on the next page
- "Configuring an Application to Use the App Gateway" on page 855

App Gateway Configuration Workflow

Here's an overview of what you need to configure for App Gateway connections:



When you configure an application to use the App Gateway, you don't have to change any configurations in the application directly. In Admin Portal, you enable the application for App Gateway access and you enter the existing URL that users enter to open the application.

At that point, you have a choice: you can use an external URL that the Privileged Access Service automatically generates for you to use, or you can continue using your existing, internal URL. In most cases, it works better for your users to use the auto-generated URL for testing purposes only and then switch over to use the existing URL for external App Gateway access for applications in production mode.

If you use the same DNS name both internally and externally, you must be able to create internal and external DNS entries that point to different things. For example:

Internal zone: Host (A) record pointing to IP address

External zone: CNAME record pointing to <guid>-gw.gateway..centrify.com

Which URL you use involves different advantages and disadvantages.

	Advantages	Disadvantages
Use the App Gateway, and use the auto-generated, external URL for App Gateway connections	Easy to configure and test Excellent for test environments	Existing links and bookmarks won't work outside of the corporate network. Users have to use different URLs depending on whether they're accessing the application internally or externally.
Use your existing, internal URL for App Gateway connections	Existing links and bookmarks work regardless of user login location. Seamless user experience. Recommended for production environments	You do more configuration: you need to upload the URL certificate and private key, and edit your DNS settings.

Configuring an Application to Use the App Gateway

On the **App Gateway** page, you can configure the application so that your users can access it whether they are logging in from an internal or external location. For applications configured for the App Gateway, users do not have to use a VPN connection to access the application remotely.

Note: App Gateway is an add-on feature. Please contact your sales representative to have the feature enabled for your account.

Note: Some applications can be used with App Gateway; not all applications are set up to use this feature. At this time, Web applications may use HTTPS or HTTP, and either the standard port of 443 or a non-standard port. IP addresses are only supported for on-premise apps and are not supported for external-facing apps.

To configure an application for external App Gateway connections

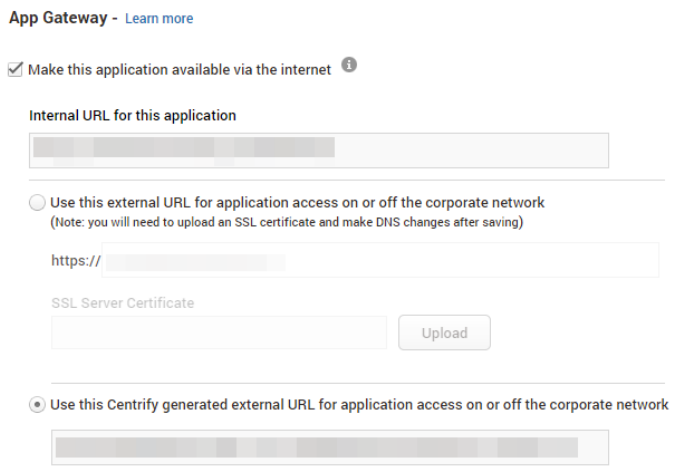
1. Make sure that your on-premise web application is accessible.

   Note: You can specify a URL that uses either HTTP or HTTPS. To specify the port, add the port at the end of the URL, such as HTTP://acme.log.com:3433. Login URLs with IP addresses are not supported.

2. Install Delinea in your network. If you have already installed them, just make sure that they're the current release version (prior versions don't support App Gateway connections). If you're using a cloud-based directory service, you won't need to install the Active Directory service components with the Delinea Connector.
3. Add, configure, and deploy the application.

   You can enable App gateway access for custom applications, such as user-password and SAML applications.
4. (Optional) On the Application Gateway page, select **Make this application available via the Internet**.

   The Privileged Access Service verifies the application settings and displays the URL that you provided in application settings as the internal URL for the application.



5. Specify the external URL that users open to access the application from external locations. You can use an existing URL or use one that the Delinea automatically generates for you.

   If you use an existing external URL, any links to the application URL do not need to change and will continue to work as is. However, you do need to upload an SSL certificate and modify your DNS settings.

   - To use your existing external URL, select **Use this external URL for application access on or off the corporate network** and do the following:

     a. Enter the existing URL. You can enter an internal or external URL here. Login URLs with IP addresses are not supported.

     b. Click **Upload** to browse to and upload your SSL certificate with the private key for the URL that you entered.

        The certificate file has either a .PFX or .P12 filename extension.

   - To use the auto-generated URL, select **Use this Delinea generated external URL for application access on or off the corporate network**. Later, you'll need to notify users to use the auto-generated URL or access the application from the Admin Portal.

     If you use the auto-generated URL, the option **Rewrite generated external URL to internal URL in requests and responses** found in **Gateway Options** is selected by default to improve compatibility with applications that utilize html redirects in the payload.

6. In **Gateway Options**, select **Lock session to source IP address** to require re-authentication if a user's source IP address changes during the app gateway session.

   This option is not recommended for OWA, as it might cause authentication failures.

7. In **Gateway Options**, select **Lock session to expiration of user** to require re-authentication if a user's identity cookie expires during the app gateway session.

   This option is not recommended for OWA, as it might cause authentication failures.

8. In **Gateway Options**, select **Pass the requested URL to the application without decoding**.

This option passes the raw URL to the application, which is sometimes necessary for compatibility.

9. In **Gateway Options**, select **Enable standard web proxy headers** to set X-Forwarded-For (RFC-7239), and REMOTE_USER.

   This option allows you to use the App Gateway with network monitoring devices or additional reverse proxies. In addition, you can select either **Client IP Address** or **Username** as values for the X-Forward-For header, depending on whether you want to monitor the header for specific IP ranges or users.

10. Select a connector to use with the application at the __Delinea Connectors to use with this service** section. Choose one of the following:

    - Any available

      Select this option to allow the Privileged Access Service to randomly select one of the available connectors for your App Gateway configuration. Click **Test Connection** to make sure the connection between the connector and the application is successful.

    - Choose

      Select this option to specify one or more Delinea Connectors to use for your App Gateway configuration. If you select more than one connector, the Privileged Access Service randomly chooses one of the selected connectors to use for the application. Once the configuration is saved, each future App Gateway request uses a random connector from those selected, as long as the connector is online.

      Once you select the connectors you want to use, click **Test Connection** to make sure the connection between the selected connectors and the application is successful. At least one connector must succeed in order to save the configuration.

      Note: If any of the Delinea Connectors are offline, they are not displayed in the list of available Delinea Connectors.

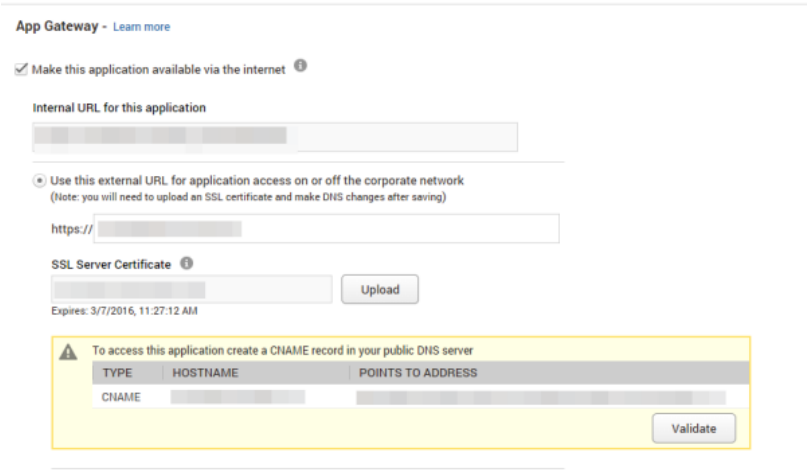
11. Click **Save** to save the App Gateway changes.

    Note: If you configured the application to use an external URL you need to edit your DNS settings to accommodate the App Gateway connection for this application. For more details, see "Adding the CNAME Record in Your Public DNS Server" below.

Adding the CNAME Record in Your Public DNS Server

When you choose to use your existing external application URL, the Privileged Access Service displays the CNAME record that you need to enter in your public DNS server. This record creates an alias so that when users enter your existing URL (host name), they're redirected automatically to the internal application (by way of the canonical name).

After you upload the certificate, Admin Portal displays the CNAME record entry that you need to enter in your DNS settings.



1. In your domain's DNS settings, you'll enter a CNAME record to map this URL to the application's gateway connection URL.
2. Afterword in the App Gateway settings, you click **Validate** to ensure that the DNS settings are correct.

App Gateway Troubleshooting

Make sure that you have the latest version of the Delinea Connector. See "How to Auto-update Connector Software" on page 421 for more information.

Using App Gateway Diagnostics

App Gateway Diagnostics generates reports that help troubleshoot problems externally accessing applications through App Gateway. App Gateway Diagnostics records web traffic metadata for the application using App Gateway for 24 hours or until you stop the diagnostics session, whichever comes first. Diagnostic reports are generated when you stop the session.

To start a Admin Portal App Gateway Diagnostics session:

1. Configure the application for external App Gateway connections. For more details, see "Configuring an Application to Use the App Gateway" on page 855.
2. On the **App Gateway** page for the application, click **Start Diagnostics**. A diagnostic sessions starts, indicated by the text **Diagnostic session running ...** .
3. Access the application through the App Gateway as you normally would.

   The diagnostic session records web traffic metadata for the application for 24 hours or until you stop the diagnostics session, whichever comes first.
4. On the **App Gateway** page, click **Stop Diagnostics** to stop the diagnostic session. Links to session reports for the most recent diagnostic session appear.
5. Click the links to view the selected report on the Reports page. The following reports are available.

- Pageloads_<appname><date time>

  The PageLoads report shows page load performance for any page in the application that a user tried to access through App Gateway during the diagnostic session.

- Urls_<appname><date time>

  The Urls report shows absolute links to application content where the hostname differs from the application's tunneled hostname. Any content appearing in this report indicates the application is not compatible with App Gateway. Include this report in any correspondence with Technical Support regarding application compatibility with App Gateway.

  When viewing the report, use the options available in the Actions menu to distribute the reports for use in any correspondence with Technical Support regarding App Gateway connection issues. See "Working with Reports" on page 1060 for more information about the Actions menu.

  
  All reports generated by App Gateway Diagnostics are available on the **Reports** page in the **Shared Reports > AppGateway** folder. See "Managing Reports" on page 1053 for more information about managing reports.

Adding Web Applications

Select an application from the following list for more information on how to configure it in the Admin Portal.

- "Amazon Web Services (SAML) Requirements for SSO" on the next page
- "Cloudera Manager" on page 865
- "CloudLock" on page 876
- "Confluence Server" on page 880
- "Dome9" on page 886
- "Jira Cloud" on page 894
- "JIRA Server (On-Premise)" on page 900
- "Palo Alto Networks" on page 911
- "Splunk" on page 918
- "Sumo Logic" on page 928

Amazon Web Services (SAML)

If you're trying to configure the Amazon Web Services: SAML app, you're in the right place.

Amazon Web Services (SAML) Requirements for SSO

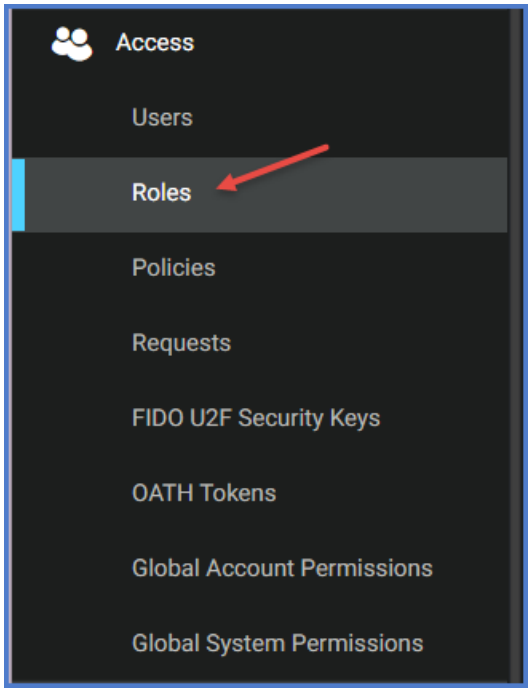
Before you configure the Amazon Web Services (AWS) web application for SSO, you need the following:

- An active Amazon Web Services account with administrator rights for your organization.
- A signed certificate. You can either download one from Admin Portal or use your organization's trusted certificate.

Adding Amazon Web Services (SAML) in Admin Portal

Creating an Amazon Web Services (SAML) user in the CentrifyAdmin Portal

1. In the Delinea Admin Portal browser window, click **Access** > **Roles**.



2. Click **Add Role**, name the new role **CentrifyAmazonSSO**, and enter a description of the role.

   Note: The role you create in the Centrify Admin Portal will need to match the role you will create in AWS IAM.

3. Click **Members**, add the members who will be using this SAML application, and click **Save**.
4. Navigate to **Apps** > **Web Apps**.
5. Click **Add Web Apps** to create a new Web App and click **Add** next to Amazon Web Services SAML.
6. Click **Add** to confirm you want to add Amazon Web Services SAML.
7. Click **Close** to close the Add Web Apps window.
8. Click on the web app you just added and navigate to **Settings**.
9. Add **Your AWS Account ID**.
10. Click **Trust** and click **Download Python and PowerShell CLI utilities to access Amazon Web Services here.** and save the file on your computer.
11. Click **Permissions**, and add the members with role permissions to use this SAML application. These are the same members added to the role from the previous steps.
12. Click **Account Mapping** for configuration details. **Directory Service field name** should be mail. See "Map User Accounts" on page 840 for more information.
13. Click **Save**.

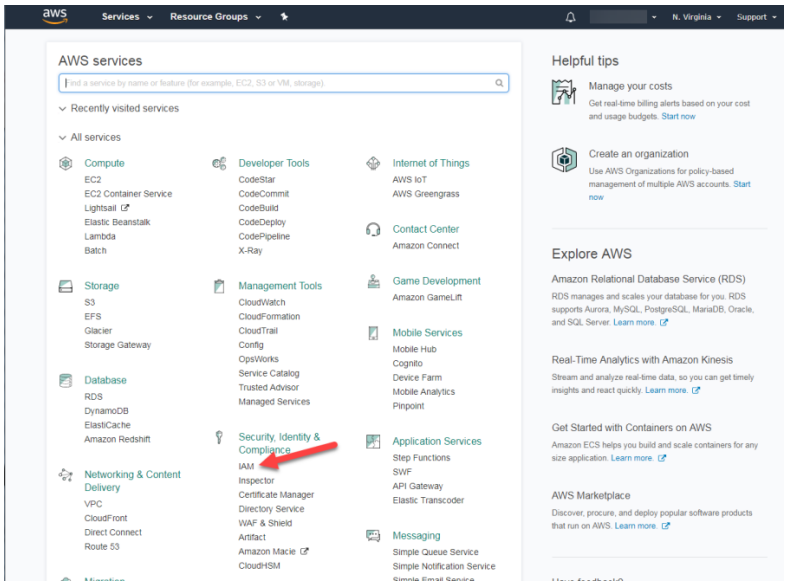
Creating a provider in Amazon Web Services

1. In your web browser, go to the following URL and sign in:

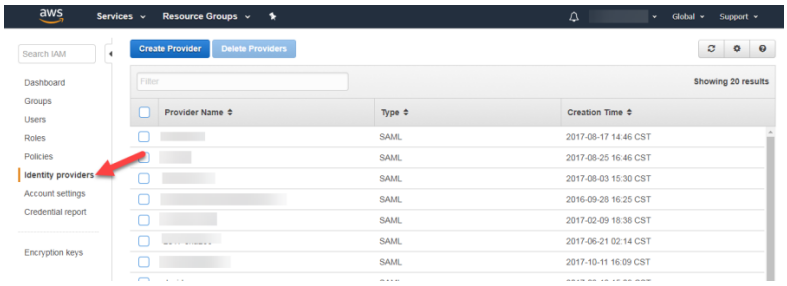
   https://aws.amazon.com.

   > **Note:** It is helpful to open the Amazon Web Services web application and the Centrify Admin Portal Trust window simultaneously to copy and paste settings between the two browser windows.

2. Under Security, Identity, & Compliance, click **IAM.**

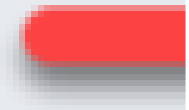


3. Click **Identity providers**.

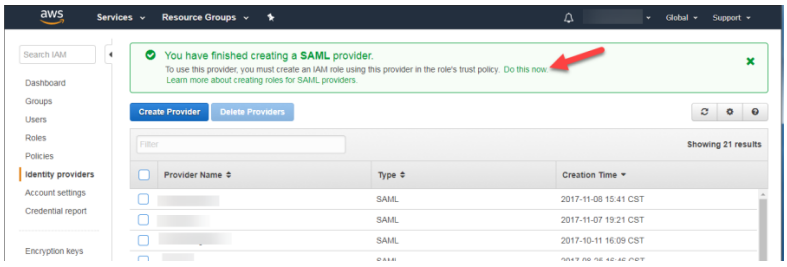


4. Click the **Create Provider** , and choose **SAML** as the provider type from the drop-down list.
5. Enter Delinea as the **Provider Name**.
6. Upload the Metadata Document downloaded during the Web App creation. On the AWS web page, click **Choose File** and select the XML file you just downloaded.
7. Click **Next Step,** and if the provider information looks right, click **Create**.
8. Configure the following settings (in the Amazon Web Services web application and in the Centrify Admin Portal).

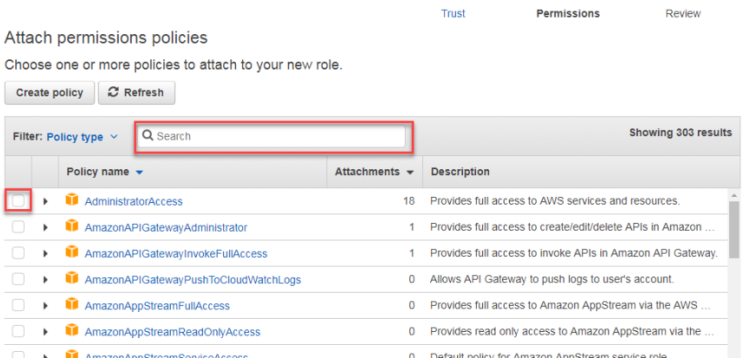
The red arrows in the table below indicate the direction of the copy and paste operation between the two windows. For instance, the first arrow in the table below indicates that you copy the content from the indicated field on the Amazon Web Services website and paste it into the corresponding field in the Privileged Access Service Admin Portal.

Admin Portal	Copy/Paste Direction	Amazon Web Services web application	What you do
Download Metadata File		Choose File	1. On the Trust page in Admin Portal, click **Download Metadata File** and save the file on your computer. 2. On the AWS web page, click **Choose File** and select the XML file you just downloaded. 3. Click **Next Step**.
AWS Account ID	N/A	N/A	Enter this value on the Settings page. To find this value log in to AWS Management Console with a Root (Admin) Account. Click on your name at top right corner and then click **My Account**. Your AWS Account ID is the Account Number below the *Sign Out* link.
Download Signing Certificate	N/A	N/A	If you use your own certificate, upload it in the Trust page in Centrify Admin Portal first. This can be done in Identity Provider Configuration > Metadata > Signing Certificate Also note that you must upload the certificate from your local storage prior to downloading the IdP metadata or the Signing Certificate from the Applications Settings page. If the IdP metadata is available from a URL, be sure to upload the certificate prior to providing the URL to your service provider.

9. Click **Do this now** in the information box at the top of the page to create an Identity and Access Management (IAM) role using this provider in the role's trust policy.



10. Select the provider you just created from the **SAML provider** drop-down list.
11. Select **Allow programmatic and AWS Management Console access**.
12. Click **Next: Permissions**.
13. **Select** the check box for the policy you want to assign to this role.



If you are not sure, select the most appropriate role from these three options:

14. Administrator Access
    - Power User Access
    - Read Only Access

    You may need to use the search box to locate your policy name.
15. Click **Next: Review.**
16. Enter a **Role name** and optionally, a **Role description.**
17. Click **Create Role**.
18. In the web app in the Delinea Admin Portal, under **SAML Response**, modify the custom logic to include the name of the role created in AWS IAM if you have more than one SAML provider. If there is only one, the default entry will suffice.

```
var v = 'arn:aws:iam::' + accountNumber + ':role/' + roleNames[i] + ',arn:aws:iam::' +
accountNumber + ':saml-provider/' + DefaultAwsSsoProviderName;

var v = 'arn:aws:iam::' + accountNumber + ':role/' + roleNames[i] + ',arn:aws:iam::' +
accountNumber + ':saml-provider/CentrifySSO';
```

Delinea Amazon Web Services CLI Utilities

Delinea offers Python and PowerShell CLI utilities to access Amazon Web Services by leveraging Privileged Access Service. The AWS CLI utilities are available from the Downloads area of the Admin Portal.

Refer to The Delinea Developer Program for more information about how to install and use the AWS CLI utilities, such as AWS Powershell Utility V10.

AWS (SAML) Specifications

Each SAML application is different. The following table lists features and functionality specific to Amazon Web Services.

Capability	Supported?	Support details
Web browser client	Yes	
Mobile client	Yes	iOS and Android
SAML 2.0	Yes	
SP-initiated SSO	No	
IdP-initiated SSO	Yes	
Force user login via SSO only	No	After SSO is enabled, users can continue to log in to Amazon Web Services with their local user name and password.
Separate administrator login after SSO is enabled	Yes	After SSO is enabled, administrators can continue to log in to Amazon Web Services with their local user name and password.
User lockout	No	
Administrator lockout	No	
Multiple User Types	Yes	Refer to Amazon Web Services documentation for details.
Self-service password	Yes	Users can reset their own passwords. Note that administrators cannot reset a user's password.
Access restriction using a corporate IP range	Yes	You can specify an IP Range in the Admin Portal Policy page to restrict access to the application.

Cloudera Manager

Cloudera Manager is an end-to-end application for managing CDH clusters. The following is an overview of the steps required to configure the Cloudera Manager Web application for single sign-on (SSO) via SAML. Cloudera Manager offers both IdP-initiated SAML SSO (for SSO access through the Admin Portal) and SP-initiated SAML SSO (for SSO access directly through the Cloudera Manager web application).

1. Prepare "Cloudera Manager Requirements for SSO" on the next page.
2. "Adding Cloudera Manager in Admin Portal" on page 867 in the Delinea Admin Portal.
3. Configure the application for single sign-on in Delinea Admin Portal and on the Cloudera Manager web site.

   You will need to copy some settings from Application Settings in Delinea Admin Portal and paste them into fields on the Cloudera Manager website, and copy some settings from the Cloudera Manager website and paste them into Delinea Admin Portal. For details, see

Cloudera Manager Requirements for SSO

Before you configure the Cloudera Manager web application for SSO, you need the following:

- Cloudera Enterprise installed.
- An active Cloudera Manager account for your organization with Full Administrator and User Administrator roles.
- A signed certificate.
- Cloudera Security expects token a signing certificate in a Java KeyStore format. You can either use the token signing certificate that is available by default for your Privileged Access Service Instance or you can upload your organization's certificate in Delinea. Once you decide which token signing certificate to use, import that certificate in a Java KeyStore file. Cloudera Manager also expects its own Private Key in the same keystore file. Cloudera Manager uses this Private Key to sign the SAML request. For more information, see: Cloudera documentation, Understanding Keystores and Truststores

Setting Up the Certificates for SSO

To establish a trusted connection between the web application and the Privileged Access Service, you need to have the same signing certificate in both the application and the application settings in Admin Portal.

If you use your own certificate, you upload the signing certificate and its private key in a .pfx or .p12 file to the application settings in Admin Portal. You also upload the public key certificate in a .cer or .pem file to the web application.

What You Need to Know About Cloudera Manager

Each SAML application is different. The following table lists features and functionality specific to Cloudera Manager.

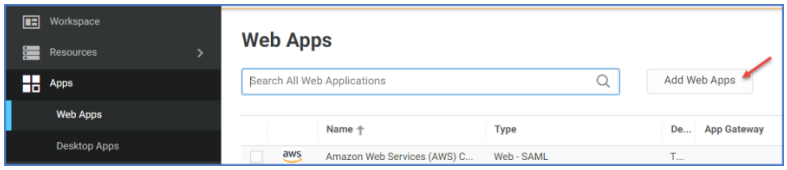
Capability	Supported?	Support details
Web browser client	Yes	
Mobile client	No	
SAML 2.0	Yes	
SP-initiated SSO	Yes	
IdP-initiated SSO	Yes	However, users can choose to disable this by unclicking **Show in User App List** in Cloudera Manager.
Force user login via SSO only	Yes	Once SAML SSO is enabled, all users are by default authenticated using SSO. However, those users who already had a password set before SSO was enabled can login using this URL: http://*<YOUR-CLOUDERA-MANAGER-FQDN>*:7180/cmf/localLogin

Capability	Supported?	Support details
Separate administrator login after SSO is enabled	Yes	After SSO is enabled, admin and other users who already have a password set or are created by the Administrator after SSO is enabled can login with this URL: http://*<YOUR-CLOUDERA-MANAGER-FQDN>*:7180/cmf/localLogin.
User or Administrator lockout risk	Yes	All external users that are created through User Provisioning will get blocked if there is any issue with the SSO integration. The only users who can log in using the alternate URL http://*<YOUR-CLOUDERA-MANAGER-FQDN>*:7180/cmf/localLogin are those who have a password already set before SSO integration, or who are created by the Administrator after SSO is enabled. Administrators can login with the alternate URL and unblock the users.
Multiple User Types	No	
Self-service password	Yes	Regular users can reset their own passwords. Admins can reset user passwords. Users created through User Provisioning cannot reset their own passwords.
Access restriction using a corporate IP range	Yes	You can specify an IP Range in the Admin Portal Policy page to restrict access to the application.

Adding Cloudera Manager in Admin Portal

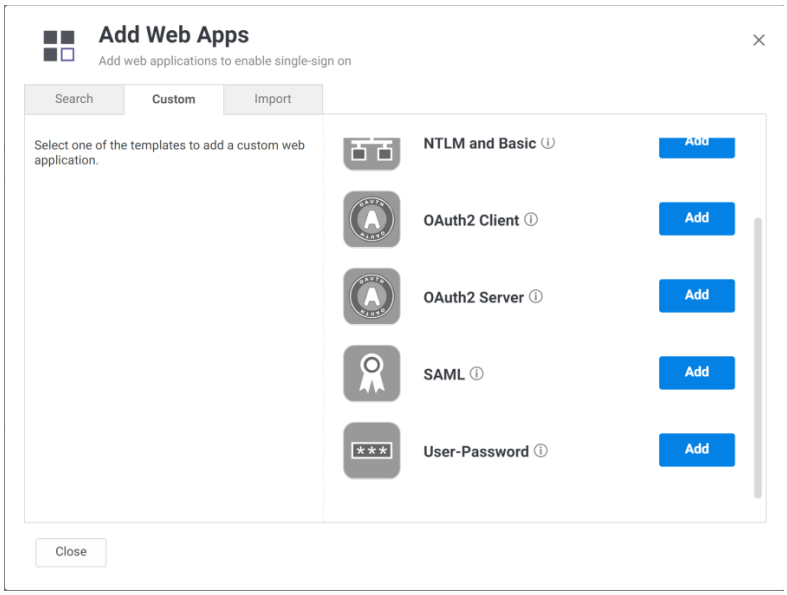
To add and configure the Cloudera Manager application in Admin Portal:

1. In Admin Portal, click **Apps**, then click **Add Web Apps**.



   The Add Web Apps screen appears.

2. On the Search tab, enter the partial or full application name in the Search field and click the search icon.

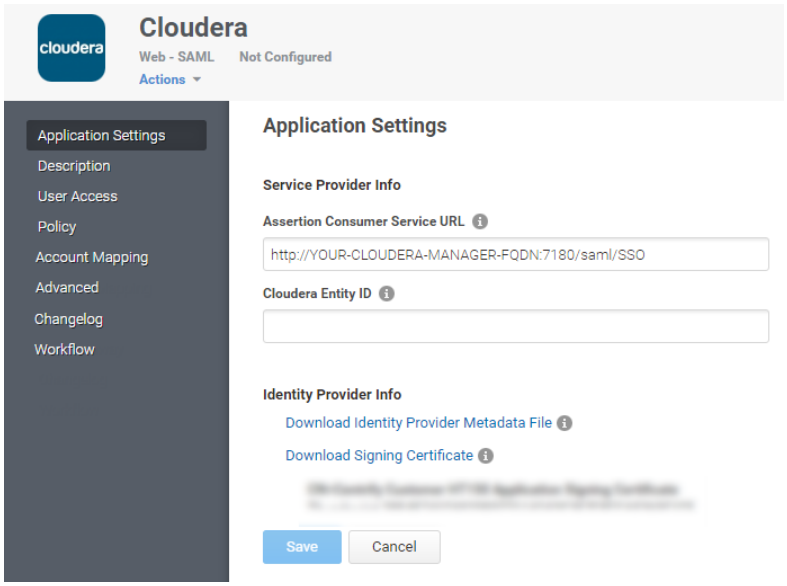


3. Next to the application, click **Add**.
4. In the Add Web App screen, click **Yes** to confirm.

   Admin Portal adds the application.
5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Application Settings page.

   Note: The description of how to choose and download a signing certificate in this document might differ slightly from your experience. See "Choose a Certificate File" on page 842 for the latest information.



6. Keep this browser tab open to the Application Settings page for the Cloudera Manager app.

Configuring Cloudera Manager for Single Sign-On

To configure Cloudera Manager for SSO

1. On the Application Settings page in Admin Portal, configure the following:

Field	Required or optional	Set it to	What you do
Assertion Consumer Service URL	Required	http://*<YOUR-CLOUDERA-MANAGER-FQDN>* :7180/saml/SSO	Replace *<YOUR-CLOUDERA-MANAGER-FQDN>* in the default URL with the fully-qualified domain name of your Cloudera Manager host.
Cloudera Entity ID	Optional	The Entity ID you chose for this instance of Cloudera Manager.	Each Cloudera Manager instance has a different entity ID. These are assigned by organizational policy and must match with the value of the **SAML Entity ID** property that you can find in Cloudera Manager at **Administrator > Settings > External Authentication**.

2. Click **Download Identity Provider Metadata File** and save the file to your computer.

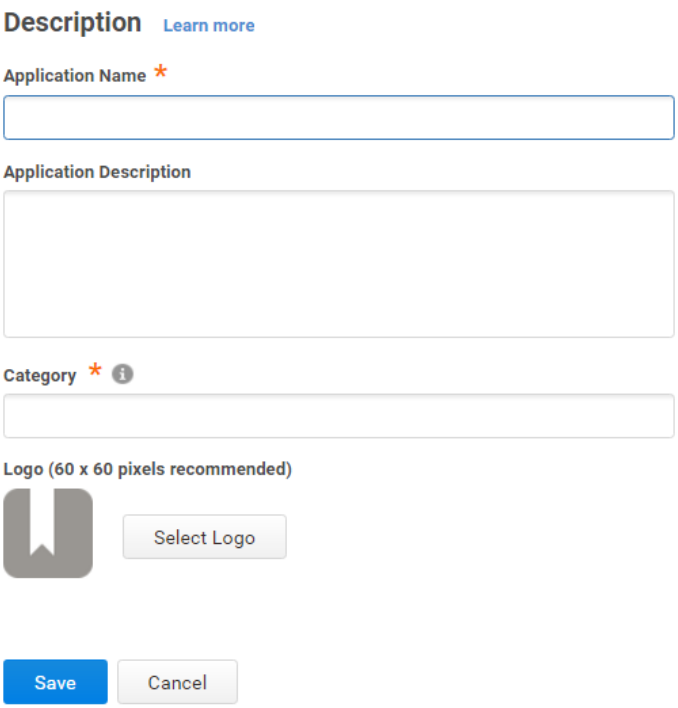
   You will need to know the path to this file when "Configuring Cloudera Manager for Single Sign-On" above.

3. (Optional) If you plan to use the Delinea signing certificate, click **Download Signing Certificate** and save the file to your computer. If you plan to use your organization's signing certificate, you can skip this step.

4. On the **Application Settings** page, expand the **Additional Options** section and specify the following settings:

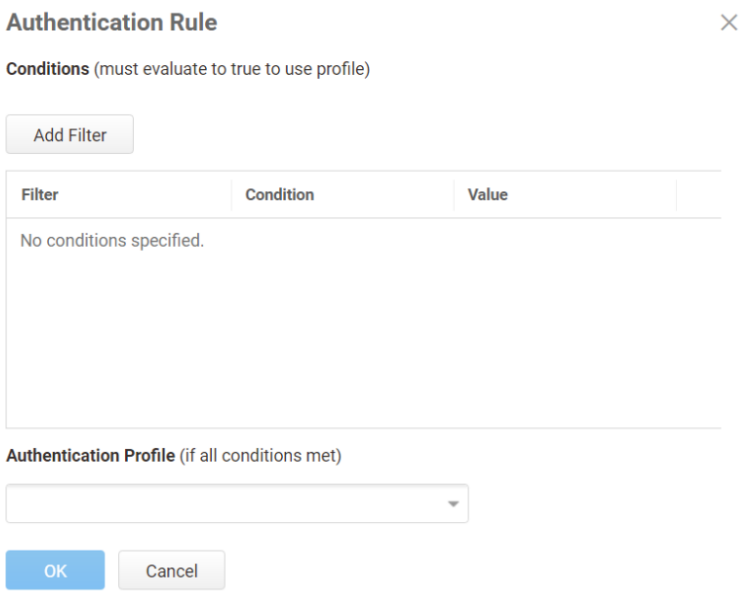
Option	Description
Application ID	Configure this field if you are deploying a mobile application that uses the Centrify mobile SDK. The Privileged Access Service uses the Application ID to provide single sign-on to mobile applications. Note the following: The Application ID has to be the same as the text string that is specified as the target in the code of the mobile application written using the mobile SDK. If you change the name of the web application that corresponds to the mobile application, you need to enter the original application name in the Application ID field. There can only be one SAML application deployed with the name used by the mobile application. The Application ID is case-sensitive and can be any combination of letters, numbers, spaces, and special characters up to 256 characters.

5. (Optional) On the **Description** page, you can change the name, description, and logo for the application. For some applications, the name cannot be modified.

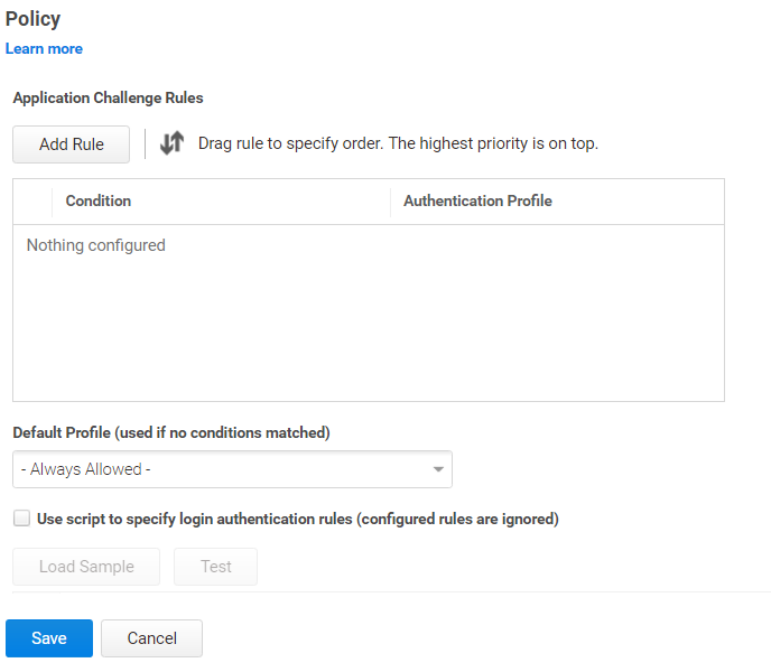


6. Click **Add Rule**.

   The Authentication Rule window displays.



7. (Optional) On the **Policy** page, specify additional authentication controls for this application.



a. Click **Add Filter** on the Authentication Rule window.

b. Define the filter and condition using the drop-down boxes. For example, you can create a rule that requires a specific authentication method when users access the Privileged Access Service from an IP address that is outside of your corporate IP range. Supported filters are:

Filter	Description
IP Address	The authentication factor is the computer's IP address when the user logs in. This option requires that you have configured the IP address range in Settings, Network, Corporate IP Range.
Identity Cookie	The authentication factor is the cookie that is embedded in the current browser by the Privileged Access Service after the user has successfully logged in.
Day of Week	The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.
Date	The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.
Date Range	The authentication factor is a specific date range.

Filter	Description
Time Range	The authentication factor is a specific time range in hours and minutes.
Device OS	The authentication factor is the device operating system.
Browser	The authentication factor is the browser used for opening the Privileged Access Service Admin Portal.
Country	The authentication factor is the country based on the IP address of the user computer.
For the Day/Date/Time related conditions, you can choose between the user's local time and Universal Time Coordinated (UTC) time.	

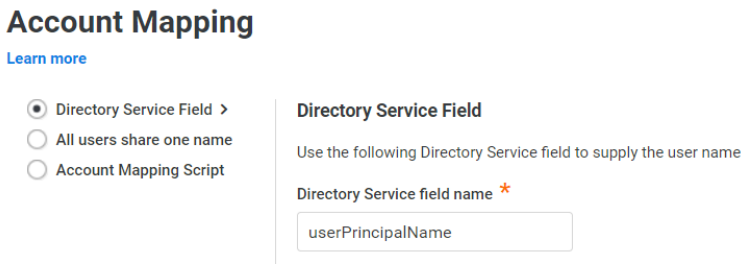
8. Click the **Add** button associated with the filter and condition.
   a. Select the profile you want applied if all filters/conditions are met in the **Authentication Profile** drop-down.

      The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the **Add New Profile** option. See Creating authen if a user does not match any of the configured conditions.

   If you have no authentication rules configured and you select **Not Allowed** in the **Default Profile** dropdown, users will not be able to log in to the service.
9. Click **Save**.

   If you have more than one authentication rule, you can prioritize them on the **Policy** page. You can also include JavaScript code to identify specific circumstances when you want to block an application or you want to require additional authentication methods. For details, see "Application Access Policies with JavaScript" on page 987.

   Note: If you left the Apps section of Admin Portal to specify additional authentication control, you will need to return to the Apps section before continuing by clicking **Apps** at the top of the page in Admin Portal.
10. On the **Account Mapping** page, configure how the login information is mapped to the application's user accounts.



The options are as follows:

- **Use the following Directory Service field to supply the user name**: Use this option if the user accounts are based on user attributes. For example, specify an Active Directory field such as *mail* or *userPrincipalName* or a similar field from the Delinea Directory.
- **Everybody shares a single user name**: Use this option if you want to share access to an account but not share the user name and password. For example, some people share an application developer account.
- **Use Account Mapping Script**: You can customize the user account mapping here by supplying a custom JavaScript script. For example, you could use the following line as a script:

  ```
  LoginUser.Username = LoginUser.Get('mail')+'.ad';
  ```

  The above script instructs the Privileged Access Service to set the login user name to the user's mail attribute value in Active Directory and add '.ad' to the end. So, if the user's mail attribute value is Adele.Darwin@acme.com then the Privileged Access Service uses Adele.Darwin@acme.com.ad. For more information about writing a script to map user accounts, see the "SAML Application Scripting" on page 1001.

11. (Optional) On the **Advanced** page, you can edit the script that generates the SAML assertion, if needed. In most cases, you don't need to edit this script. For more information, see the "SAML Application Scripting" on page 1001.

    Note: By default, the script provides a list of roles that correspond to the roles set by the user. These roles are the default external facing names given to the actual Cloudera Manager roles. If you change the external facing names in Cloudera Manager SAML settings, then you should also change the role names in the script here.

    Note: This integration asserts the identity of the user in the SAML assertion through the SAML subject. If you change the option at Cloudera Manager SAML setting to Attribute then you must modify this script to provide the username information in the SAML attribute. The name of the attribute in that case must match the name configured in the Cloudera Manager SAML settings. Refer to "Configuring Cloudera Manager for Single Sign-On" on page 869 for more details.

12. (Optional) On the **Changelog** page, you can see recent changes that have been made to the application settings, by date, user, and the type of change that was made.
13. (Optional) Click **Workflow** to set up a request and approval work flow for this application.

    See "Managing Application Access Requests" on page 794 for more information.
14. Click **Save**.

Configuring Single Sign-On in Cloudera Manager

Note:This section assumes that you have two browser tabs open so that you can copy and paste information back and forth between the two tabs as appropriate:

- One tab open to the Application Settings page for the Cloudera Manager app in Delinea Admin Portal as described in "Adding Cloudera Manager in Admin Portal" on page 867. If this tab was accidentally closed, you can return to it by navigating to the Delinea Admin Portal and opening the Cloudera Manager app.
- Another tab open to the Cloudera Manager web page as you are instructed below.

To configure Cloudera Manager for SSO:

1. Open a new tab in your web browser.
2. Go to the following URL and sign in as Admin:

   https://**<YOUR-CLOUDERA-MANAGER-FQDN>**:7180/cmf/localLogin
3. Go to **Administration > Settings.**
4. In the left-hand frame, select **External Authentication**, and then select **SAML** as the External Authentication Type.
5. Scroll down to **Path to SAML IDP metadata file** and enter the path name to the metadata file you downloaded from the Application Settings page in Delinea Admin Portal.
6. Create a Java KeyStore file on the Cloudera Manager host. Import your chosen certificate file into the Java KeyStore file. Cloudera Manager also expects its Private Key imported in the same KeyStore file. Note the following:
   - The value of the KeyStore password.
   - The alias under which Cloudera Manager's private key is placed.
   - The Private key password.

For more information about how to set up the keystore file, see Cloudera documentation, Understanding Keystores and Truststores

1. Copy and paste the path of the Java KeyStore file into the **Path to SAML keystore file** field.
2. Configure the following:

Field	Required or optional	Set it to	What you do
SAML keystore password	Required	The password used to prepare the keystore	Copy/paste the keystore password in this field

Field	Required or optional	Set it to	What you do
Alias of SAML sign/encrypt Private key	Required	The sign/encrypt private key alias	Copy/paste the sign/encrypt private key alias in this field
SAML sign/encrypt Private key password	Required	The sign/encrypt private key password	Copy/paste the sign/encrypt private key password in this field
SAML Entity ID	Required	The Entity ID used on the Application Settings page in Delinea Admin Portal	Enter the value of the Cloudera Entity ID field from the Application Settings page in Delinea Admin Portal
SAML response binding	Required	HTTP-Post	Select the **HTTP-Post** option.
Source of user ID in SAML response	Required	NameID or the attribute of your choice	Enter NameID or the attribute of your choice. If you choose another attribute than NameID, you will have to update the SAML script on the Advanced page in Delinea Admin Portal to match the attribute you have chosen.
SAML attribute identifier for User Role	Required	Selected	Select this option and enter an identifier to pass to this attribute in SAML response. Choose role as the attribute name.
SAML Attribute Values for Roles	Optional	External facing names for Cloudera Manager user roles	Use the defaults or enter your custom user role names.

3. Click **Save** to save the settings.
4. Log out of your Cloudera Manager account.

For More Information about Cloudera Manager

For more information about configuring Cloudera Manager for SSO, contact Cloudera Manager support.

CloudLock

With Privileged Access Service, you can choose single-sign-on (SSO) access to the CloudLock web application with IdP-initiated SAML SSO (for SSO access through the Admin Portal) or SP-initiated SAML SSO (for SSO access directly through the CloudLock web application) or both. Providing both methods gives you and your users maximum flexibility.

If CloudLock is the first application you are configuring for SSO through Privileged Access Service, read these topics before you get started:

- "Introduction to Application Management" on page 823
-

CloudLock SSO requirements

Before you configure the CloudLock web application for SSO, you need the following:

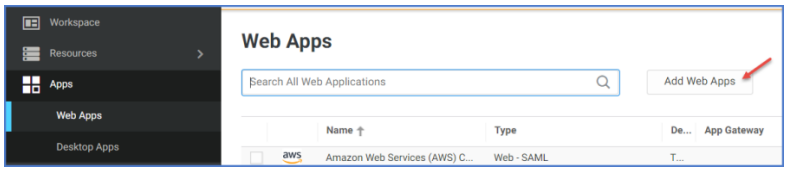
- An active CloudLock account with administrator rights for your organization.
- An Assertion Consumer Service URL from CloudLock.
- A signed certificate.
- You can either download one from Admin Portal or use your organization's trusted certificate.

Adding and configuring CloudLock in Admin Portal

Tip: It is helpful to open Centrify Admin Portal Application Settings and the CloudLock web application simultaneously to copy and paste content between the two browser windows. For information on how to access the CloudLock web application, see "Configuring CloudLock for SSO" on page 878.

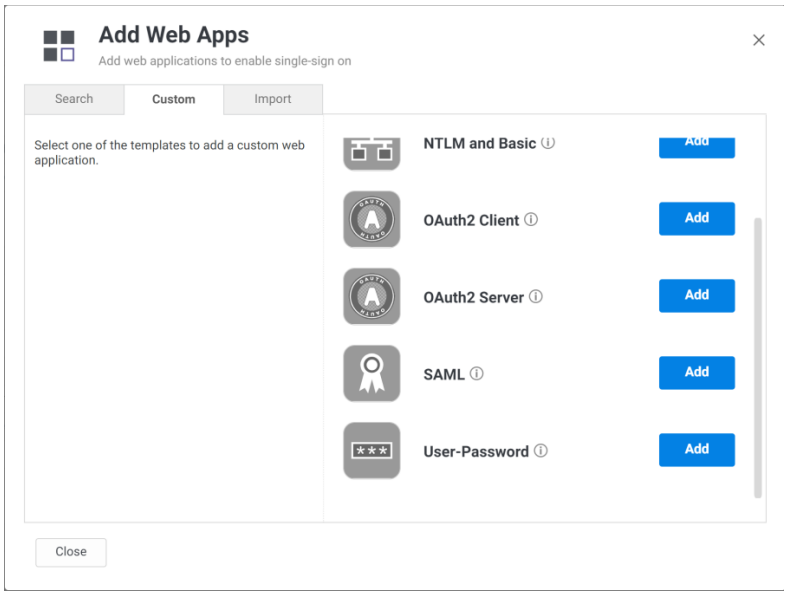
To add and configure the CloudLock application in Admin Portal:

1. In Admin Portal, click **Apps**, then click **Add Web Apps**.



   The Add Web Apps screen appears.

2. On the Search tab, enter the partial or full application name in the Search field and click the search icon.



3. Next to the application, click **Add**.
4. In the Add Web App screen, click **Yes** to confirm.

   Admin Portal adds the application.

5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Settings page.

   Note: The description of how to choose and download a signing certificate in this document might differ slightly from your experience. See "Choose a Certificate File" on page 842 for the latest information.

6. Configure the following:

Field	Required or optional	Set it to	What you do
Assertion Consumer Service (ACS) URL	Required	Your CloudLock provided ACS URL.	Enter the ACS URL you received from CloudLock. For example, https://platform.cloudlock.com/gate/saml/sso/acme.com where acme.com is a customer-specific account name.
Download Identity provider metadata	Required	The Privileged Access Service automatically generates the content for this field.	Click the link to download the metadata file. Open the Identity provider metadata file in a text editor and copy the content. See "Configuring CloudLock for SSO" below to complete the configuration.
Download Signing Certificate	Optional (the certificate is part of the Identity provider metadata)	The Privileged Access Service automatically generates the content.	If necessary, click the link to download the default Signing Certificate. The certificate content is automatically included as part of the Identity provider metadata. To use a certificate with a private key (pfx file) from your local storage, see below. If you replace the certificate, download the Identity provider metadata again and submit the new file to the CloudLock website (see above).

Configuring CloudLock for SSO

The following steps are specific to the CloudLock application and are required in order to enable SSO for CloudLock. For information on optional Delinea Admin Portal configuration settings that you may wish to customize for your app, see "Optional Configuration Settings" on page 844.

To configure CloudLock for SSO:

1. In your web browser, go to your CloudLock login URL and sign in with your administrator account credentials.
2. Click **Settings > Authentication and API** and enable **SAML Login.**
3. Paste the content you copied from the Identity provider metadata field in **Admin Portal > Application Settings** to the CloudLock Identity provider metadata input field.
4. Click **Submit** to save the changes.

For More Information About CloudLock

For more information about configuring CloudLock for SSO, contact CloudLock Support.

CloudLock Specifications

Each SAML application is different. The following table lists features and functionality specific to CloudLock.

Capability	Supported?	Support details
Web browser client	Yes	
Mobile client	No	
SAML 2.0	Yes	
SP-initiated SSO	Yes	Users may go directly to the CloudLock URL and then use the Privileged Access Service SSO to authenticate.
IdP-initiated SSO	Yes	Users may use SSO to log in to CloudLock through the Admin Portal.
Force user login via SAML only	No	
Separate administrator login after SSO is enabled	No	
User or Administrator account lockout risk	No	Users can log in using other SSO methods, such as Office365.
Automatic user provisioning	No	
Multiple User types	Yes	
Self-service password	No	
Access restriction using a corporate IP range	Yes	You can specify an IP Range in the Admin Portal Policy page to restrict access to the application.

Confluence Server

With Privileged Access Service, you can choose single-sign-on (SSO) access to the Confluence web application with SP-initiated SAML SSO for SSO access directly through the Confluence web application). Enabling both methods ensures that users can log in to Confluence Server in different situations such as clicking through a notification email.

Confluence does not support SAML, but it accepts a custom plugin for individual companies to modify the authentication process to their own needs, including implement Single Sign-On. A custom plugin is a set of .jar files that are implemented using Atlassian's Seraph library, and will be deployed in the Confluence Server. A system administrator must change the Confluence configuration to use the plugin.

For more information about Single Sign-on Integration with JIRA and Confluence, see Confluence documentation.

With Delinea Confluence SAML plugin deployed in Confluence Server, any unauthenticated access to Confluence resources will be redirected to Delinea Admin Portal for authentication. After that, users will be redirected back to the requested resources.

Delinea Confluence SAML plugin has been tested in Confluence Server versions 5.6.6 and 6.1.2.

If Confluence is the first application you are configuring for SSO through Privileged Access Service, read these topics before you get started:

- "Introduction to Application Management" on page 823
-

Confluence Server SSO Requirements

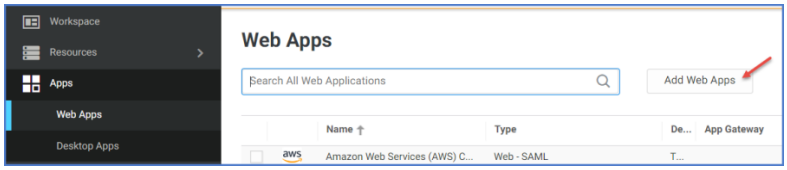
Before you configure the Confluence Server web application for SSO, you need the following:

- A Confluence Server (On-Premise).
- A system administrator account to the Confluence Server computer to deploy and configure the plugin.

Configuring Confluence Server in Admin Portal

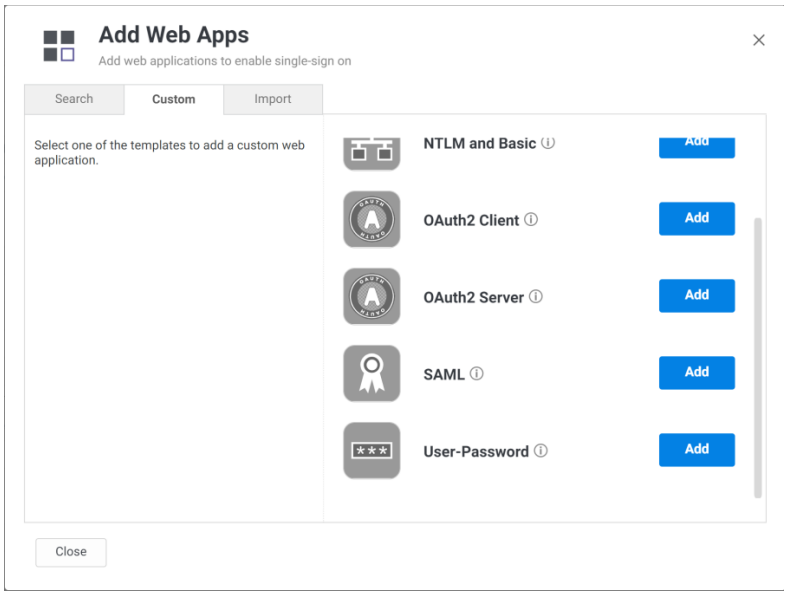
To add and configure the Confluence Server application in Admin Portal:

1. In Admin Portal, click **Apps**, then click **Add Web Apps**.



   The Add Web Apps screen appears.

2. On the Search tab, enter the partial or full application name in the Search field and click the search icon.



3. Next to the application, click **Add**.
4. In the Add Web App screen, click **Yes** to confirm.

   Admin Portal adds the application.
5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Application Settings page.

   Note: The description of how to choose and download a signing certificate in this document might differ slightly from your experience. See "Choose a Certificate File" for the latest information.
6. Configure the following:

Field	Set it to	What you do
Assertion Consumer Service URL	Your Confluence Server host and port number.	Replace YOUR-CONFLUENCE-HOST-AND-PORT with your Confluence Server host and port number, if any. For example, if your Confluence Server URL is: https://confluence.acme.com:8443 Replace YOUR-CONFLUENCE-HOST-AND-PORT with confluence.acme.com:8443. **Note**: If your Confluence Server is hosted over HTTP, change https to http.

Note: For information on optional Delinea Admin Portal configuration settings that you may wish to customize for your app, see "Optional Configuration Settings".

Downloading the Delinea Confluence SAML plugin and signing certificate

To download the plugin and certificate:

1. Go to the **Application Settings** page for the Confluence Server app in Admin Portal.
2. Copy your **IdP Issuer** and save it where you can find it in the next step.

3. Copy your **IdP Post URL** and save it where you can find it in the next step.
4. Click **Download Signing Certificate** and save the .cer file where you can find it in the next step.
5. Click **Download this plugin to be installed into your Confluence Server instance** to download a .zip file containing the SAML plugin files, and save the file where you can find it in the next step.

Deploying and configuring Confluence SAML plugin in Confluence Server

Note: These instructions assume:

- Confluence on Windows.
- Your Confluence Server is installed at: C:\Program Files\Atlassian\Confluence.

To deploy and configure the Confluence SAML plugin:

1. Access the server hosting Confluence.
2. Stop the Confluence application. For example, in Windows 7, go to **Control Panel > Administrative Tools > Services**, then right-click **Atlassian Confluence** the service and select **Stop**.

   Note: The following instructions assume that your Confluence Server is located in C:\Program Files\Atlassian\Confluence. If you choose to specify a different location, substitute that location for C:\Program Files\Atlassian\Confluence from here forward.
3. Copy the .cer signing certificate file downloaded in the previous step and place it in:

   C:\Program Files\Atlassian\Confluence\confluence\WEB-INF.
4. Copy the .zip file downloaded in the previous step and place it in a temporary location (any location other than where it will be moved to in the next few steps).
5. Extract the .zip file.

   You will get a `readme` file and a lib directory containing several .jar files.
6. Copy all the .jar files and paste them in:

   C:\Program Files\Atlassian\Confluence\confluence\WEB-INF\lib
7. Go to C:\Program Files\Atlassian\Confluence\confluence\WEB-INF\classes\seraph-config.xml.
8. Comment out the line with: <authenticator class= that is not commented out.
9. **Below** that line add the following lines:

   <!-- Centrify SAML -->

   <authenticator class="com.centrify.cloud.saas.confluencesaml.SamlAuthenticator"/>
10. Save seraph-config.xml.
11. Open C:\Program Files\Atlassian\Confluence\confluence\WEB-INF\web.xml.
12. Find the last <servlet> defined.
13. Place your cursor **below** the last <servlet> defined, then copy/paste the following:

    <!-- Centrify SAML -->

<servlet>

<servlet-name>samlServlet</servlet-name>

<servlet-class>com.centrify.cloud.saas.confluencesaml.SamlServlet</servlet-class>

<init-param>

<param-name>idpIssuerName</param-name>

<param-value><!-- Copy IdP Issuer from Application Settings in Privileged Access Service and paste it here. --></param-value>

</init-param>

<init-param>

<param-name>idpCertFile</param-name>

<param-value><!-- Absolute file path to your signing certificate file --></param-value>

</init-param>

<init-param>

<param-name>audience</param-name>

<!-- After setting the audience value below, make sure you also set the same audience value in Admin Portal. -->

<param-value>Confluence</param-value>

</init-param>

<load-on-startup>1</load-on-startup>

</servlet>

14. Set the <param-value> of idpIssuerName to the **IdP Issuer** that you copied from your Confluence Server SAML application in the previous step.
15. Set the <param-value> of idpCertFile to the absolute file path to your signing certificate file. If you used the recommended path name and if your certificate file is named Confluence.cer, you would set <param-value> to:

    C:\Program Files\Atlassian\Confluence\Confluence.cer.

    As shown here:

    <init-param>

    <param-name>idpCertFile</param-name>

    <param-value>C:\Program Files\Atlassian\Confluence\confluence\WEB-INF\Confluence.cer<param-value>

    </init-param>
16. Find the last <servlet-mapping> defined.
17. Place your cursor **below** the last <servlet-mapping> and copy/paste the following:

    <!-- Centrify SAML -->

    <servlet-mapping>

<servlet-name>samlServlet</servlet-name>

<url-pattern>/saml</url-pattern>

</servlet-mapping>

18. Find the last <filter> defined.
19. **Below** the last <filter> add the following lines:

    <!-- CentrifySAML -->

    <filter>

    <filter-name>samlFilter</filter-name>

    <filter-class>com.centrify.cloud.saas.confluencesaml.SamlFilter</filter-class>

    <init-param>

    <param-name>idpPostUrl</param-name>

    <param-value></param-value>

    </init-param>

    <init-param>

    <param-name>spIssuerName</param-name>

    <param-value>Confluence</param-value>

    </init-param>

    <init-param>

    <param-name>allowedURIs</param-name>

    <param-value>

    /saml,

    /plugins/servlet/applinks/*,

    /plugins/servlet/oauth/*,

    /rest/*

    </param-value>

    </init-param>

    </filter>

20. Set the <param-value> of idpPostUrl by copying the **IdP Post URL** from your Confluence Server SAML application in Admin Portal and pasting it inside <param-value></param-value> in the code you added in .
21. **Above** the <filter-mapping> with the <filter-name> of login, add the following lines:

    <!-- CentrifySAML -->

    <filter-mapping>

    <filter-name>samlFilter</filter-name>

<url-pattern>/*</url-pattern>

</filter-mapping>

22. Save web.xml.
23. Start the Confluence application. For example, in Windows 7, go to **Control Panel > Administrative Tools > Services**, then right-click **Atlassian Confluence** the service and select **Start**.

    Wait a few minutes for the service to start. The new settings that you just configured will be used after Confluence starts.

    Note: After configuration for SP-initiated SSO is complete, the Confluence application is automatically ready to link to other Atlassian apps released in that have also been configured for SP-initiated SSO. For information about how to link the apps, see:

    Note: You can add additional paths to the list of <param-value> values for allowedURIs in the web.xml file for Atlassian apps released in Privileged Access Service Cloud 17.10 or later. It is important that you do not change the /saml <param-value>.

For More Information About Confluence Server

- Single Sign-on Integration with JIRA and Confluence:
- https://confluence.atlassian.com/display/DEV/Single+Sign-on+Integration+with+JIRA+and+Confluence
- For configuration between Delinea SAML Plug-in and Confluence Server, contact Delinea Support.

Confluence Server Specifications

Each SAML application is different. The following table lists features and functionality specific to Confluence Server.

Capability	Supported?	Support details
Web browser client	Yes	
Mobile client	No	
SAML 2.0	Yes	
SP-initiated SSO	Yes	
IdP-initiated SSO	Yes	
Force user login via SSO only	Yes	
Separate administrator login after SSO is enabled	No	

Capability	Supported?	Support details
User or Administrator lockout risk	Yes	Because SP-initiated SSO always redirects users to Delinea and disables the function of Confluence login pages, users run the risk of being locked out of Confluence.
Automatic user provisioning	No	
Multiple User Types	Yes	SSO works the same way for all admin and non-admin user types.
Self-service password	Yes	Users can reset their own passwords. Resetting another user's password requires administrator rights.
Access restriction using a corporate IP range	Yes	

Dome9

Dome9 delivers full visibility, control and faster time to protection as organizations scale in AWS, Azure, and Google Cloud environments.

With Privileged Access Service, you can choose single-sign-on (SSO) access to the Dome9 web application with IdP-initiated SAML SSO (for SSO access through the Admin Portal) or SP-initiated SAML SSO (for SSO access directly through the Dome9 web application) or both. Providing both methods gives you and your users maximum flexibility.

Note: SP-initiated SSO for Dome9 is automatically enabled when the SAML feature is activated.

If Dome9 is the first application you are configuring for SSO through Privileged Access Service, read these topics before you get started:

- "Introduction to Application Management" on page 823
-

Dome9 requirements:

Before you configure the Dome9 web application for SSO, you need the following:

- An active Dome9 account in the Super User role.
- An additional user enabled for SSO and in the Super User role.

This is necessary because making the account owner an SSO user creates the risk of account lockout if there is an SSO failure. Specifying a different user as the SSO user ensures that you can always log in as the account owner, as long as you have the password.

- A signed certificate.

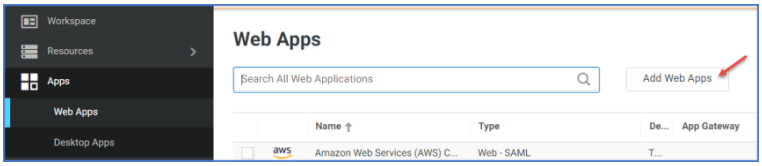
  You can either download one from Admin Portal or use your organization's trusted certificate.

Configuring Dome9 for single sign-on

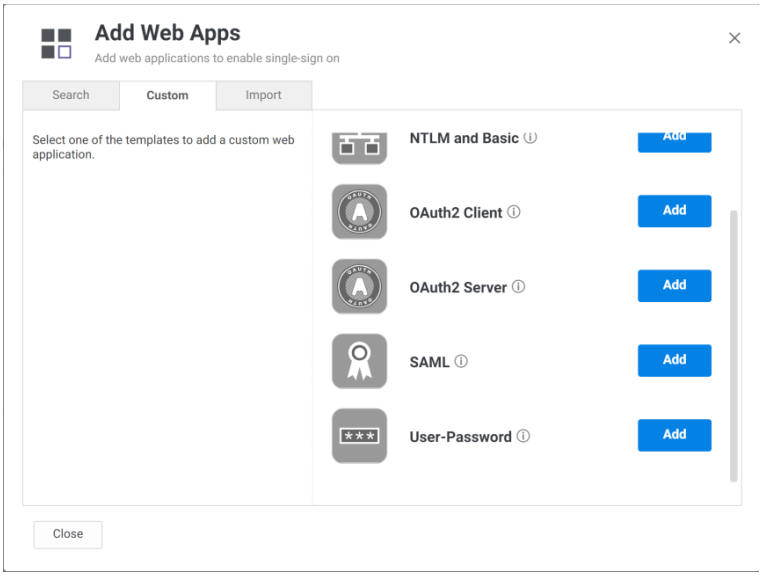
The following steps are specific to this application and are required in order to enable SSO. For information on optional configuration settings available in the Centrify Admin Portal, see "Optional Configuration Settings" on page 844.

1. Add the Dome9 application in Admin Portal.
   a. In the Admin Portal, select **Apps > Web Apps**, then click **Add Web Apps**.

      The Add Web Apps screen appears.



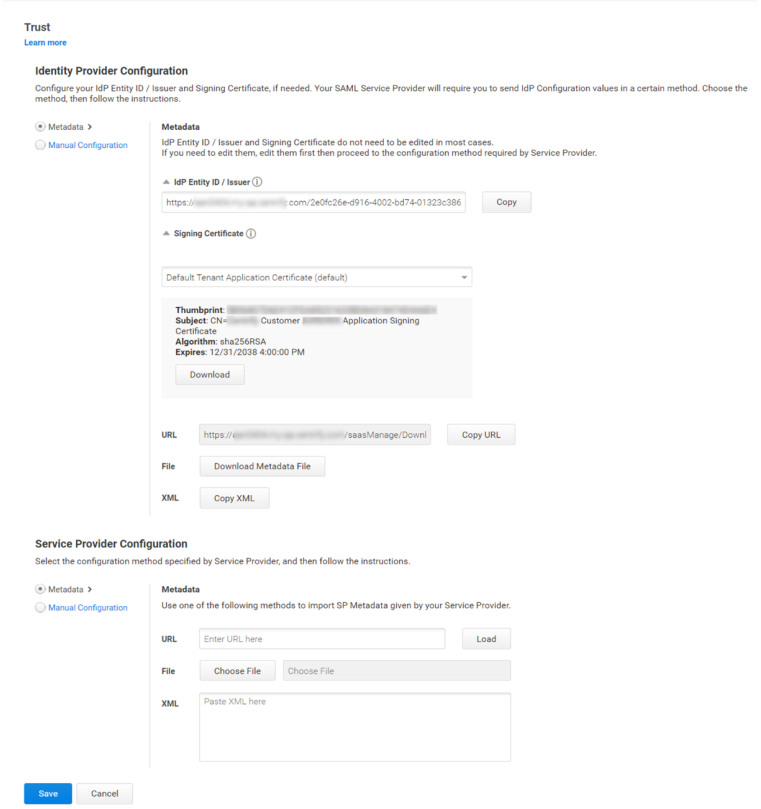
   b. On the Search tab, enter the partial or full application name in the **Search** field and click the search icon.



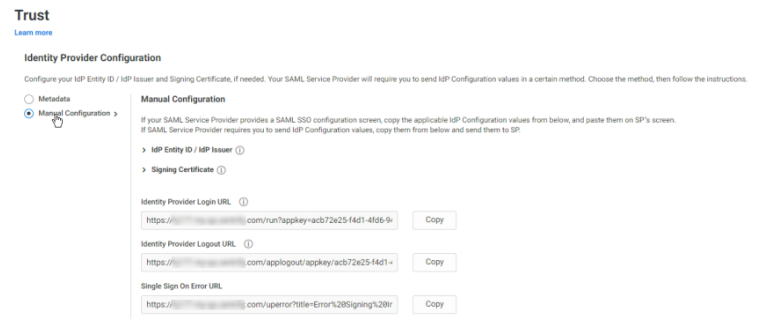
   c. Next to the application, click **Add**.
   d. In the Add Web App screen, click **Yes** to confirm.
   e. Click **Close** to exit the Application Catalog.

      The application that you just added opens to the Settings page.

f. Click the **Trust** page to begin configuring the application.



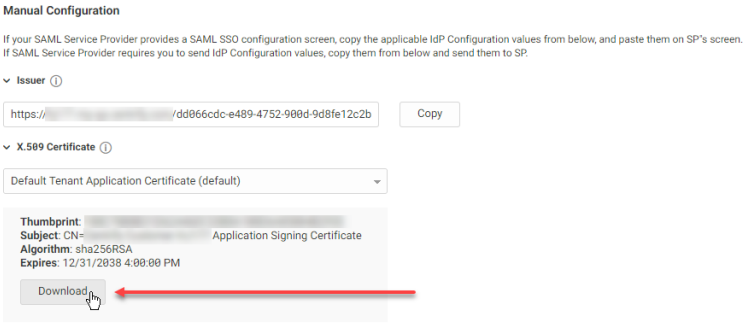
The UI is evolving in order to simplify application configuration. For example, many of the settings previously found on the Application Settings page are now on the Trust page. You might have to select **Manual Configuration** to expose those settings, as shown in the following example.



Any previously configured applications retain their configuration and do not require reconfiguration. If you are configuring an application for the first time, refer to the Trust page for any settings previously found on the Application Settings page.

In addition, the description of how to choose and download a signing certificate in this document might differ slightly from your experience. See "Choose a Certificate File" on page 842 for the latest information.

2. In the Identity Provider Configuration area of the Trust page, expand the certificate area and select the certificate that you want to use for the application, then click **Download**.



3. Open a new tab in your web browser.

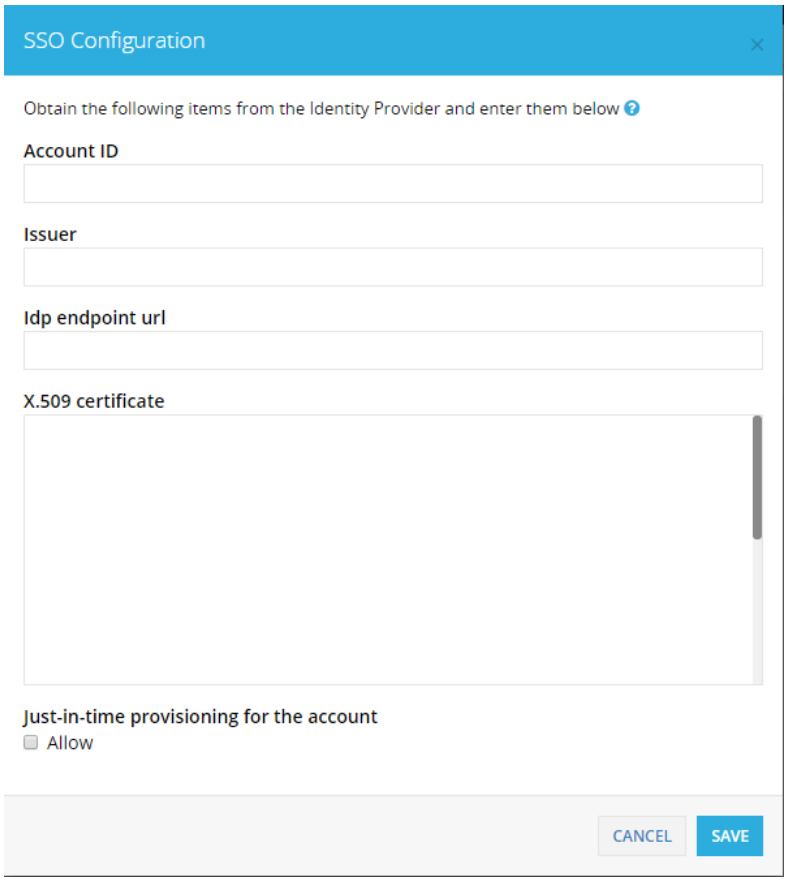
   Note: It is helpful to open the Dome9 web application and the CentrifyAdmin Portal simultaneously to copy and paste settings between the two browser windows.

4. Go to the following URL and sign in as a super user:

   https://secure.dome9.com/v2/login

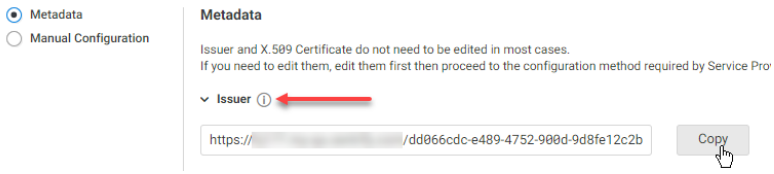
5. In the Dome9 admin portal, go to **Administration > Account Settings**, then click **SSO**.
6. Click **Enable**.

   The SSO Configuration screen appears.



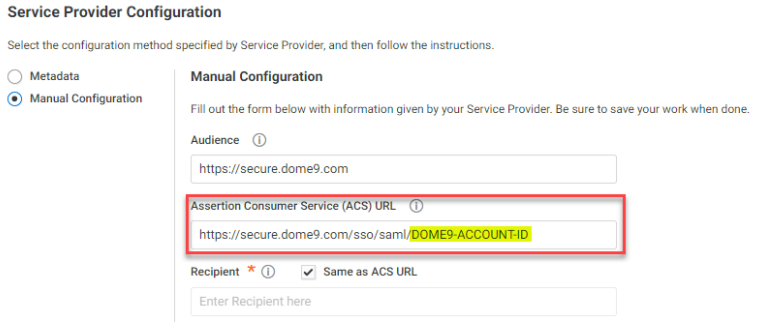
7. Open the certificate that you downloaded earlier in a text editor, then copy the contents and paste them into the web application's certificate field.
8. Enter a value in the Account ID field.

   You can use any string as long as it does not include a period or @ symbol. You will use the Account ID later to form the ACS URL.
9. In the Identity Provider Configuration area of the Trust page, expand **Issuer** and then click **Copy** to copy the **Issuer** value, then paste it in the Issuer field in the Dome9 SSO Configuration.



10. In the Identity Provider Configuration > Manual Configuration area of the Trust page, copy the **Idp endpoint url** value and then paste it in the **Idp endpoint url** field in the Dome9 SSO Configuration.

11. In the Service Provider Configuration > Manual Configuration area of the Trust page, replace the DOME9-ACCOUNT-ID portion of the ACS URL with the Account ID value you entered in the Dome9 SSO Configuration screen.



12. Deploy the application by setting permissions on the application or by adding the application to a set.

    Set permissions on the application.

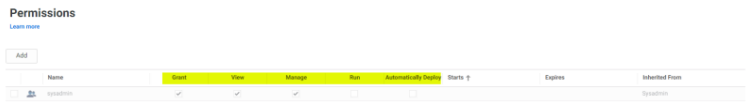
    a. On the Permissions page, click **Add**.

       The Select User, Group, or Role window appears.

    b. Select the user(s), group(s), or role(s) that you want to give permissions to, then click **Add**.

       The added object appears on the Permissions page with View, Run, and Automatically Deploy permissions selected by default.

    c. Select the desired permissions, then click **Save**.



    Add the application to a set.

    d. Add the application to an appropriate set.

       You can either create a new set or add the application to an existing set. Refer to "Managing Application Sets" on page 830 for more information about creating and modifying application sets.

    e. In the Sets section, right-click a set name, then click **Modify**.

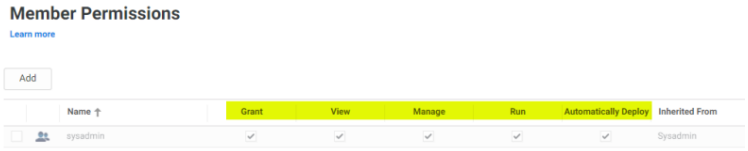
    f. On the Member Permissions page, click **Add**.

       The Select User, Group, or Role window appears.

g. Select the user(s), group(s), or role(s) that you want to give permissions to, then click **Add**.

The added object appears on the Permissions page with View, Run, and Automatically Deploy permissions selected by default.

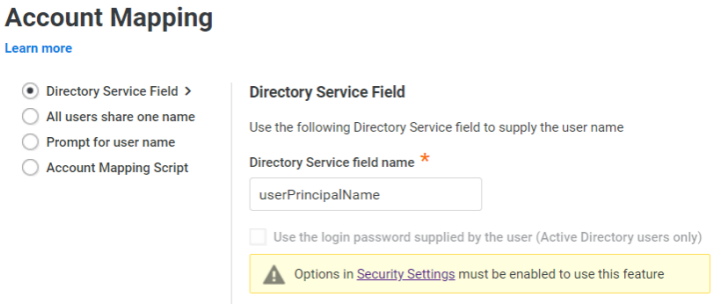
h. Select the desired permissions, then click **Save**.



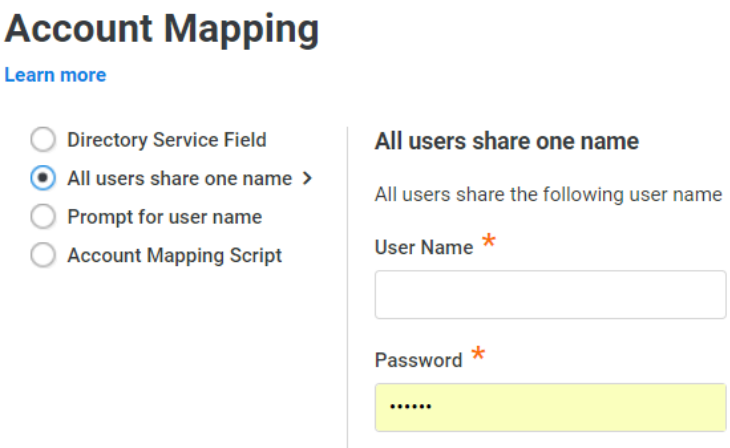
13. On the Account Mapping page, configure how the login information is mapped to the application's user accounts.

Depending on your application, available options might vary slightly.

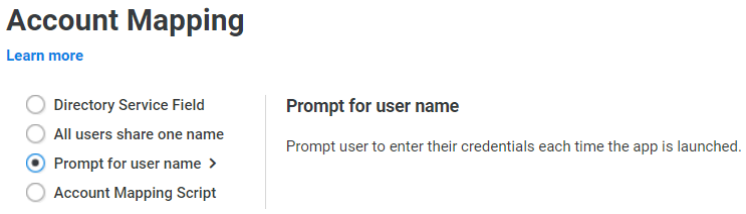
- **Directory Service Field**: Use this option if the user accounts are based on user attributes. For example, specify an Active Directory field such as *mail* or *userPrincipalName* or a similar field from the Centrify Directory.



- **All users share one name**: Use this option if you want to share access to an account but not share the user name and password. For example, some people share an application developer account.



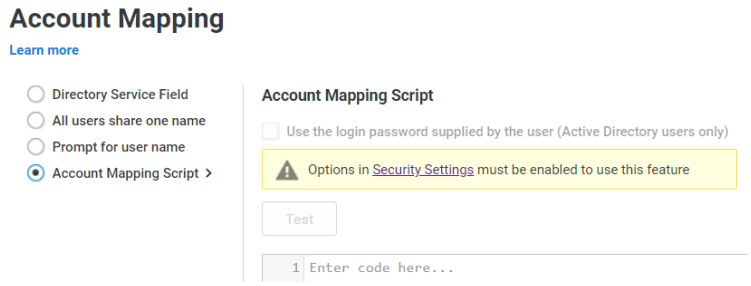
- **Prompt for user name:** Use this option if you want users to supply their own user name and password. This option only applies to user password application types. The first time that users launch the application, they enter their login credentials for that application. The Centrify Directory stores the user name and password so that the next time the user launches the application, the Centrify Directory logs in the user automatically.



- **Account Mapping Script**: You can customize the user account mapping here by supplying a custom JavaScript. For example, you could use the following line as a script:

  ```
  LoginUser.Username = LoginUser.Get('mail')+'.ad';
  ```

  The script sets the login user name to the user's mail attribute value in Active Directory and adds '.ad' at the end. For example, if the user's mail attribute value is Adele.Darwin@acme.com then the account mapping script sets LoginUser.Username to Adele.Darwin@acme.com.ad. For more information about writing a script to map user accounts, see the "SAML Application Scripting" on page 1001.



14. Click **Save** in both the Admin Portal and Dome9's SSO Configuration screen.

Dome9 Specifications

Each SAML application is different. The following table lists features and functionality specific to Dome9.

Capability	Supported?	Support details
Web browser client	Yes	
Mobile client	No	Although Dome9 offers a mobile application, SSO is not supported.
SAML 2.0	Yes	
SP-initiated SSO	Yes	

Capability	Supported?	Support details
IdP-initiated SSO	Yes	
Force user login via SSO only	Yes	
Separate administrator login after SSO is enabled	Yes	
User or Administrator lockout risk	Yes	SSO users do not get a password; SSO failure would lockout SSO users.
Just-In-Time provisioning	No	
Multiple User Types	Yes	You might need to add users with SSO enabled.
Self-service password	No	

Jira Cloud

With Delinea as your Privileged Access Service, you can choose single-sign-on (SSO) access to the Jira Cloud web and mobile applications with IdP-initiated SAML SSO (for SSO access through the Admin Portal) or SP-initiated SAML SSO (for SSO access directly through the Jira Cloud web application) or both. Providing both methods gives you and your users maximum flexibility.

If Jira Cloud is the first application you are configuring for SSO through Privileged Access Service, read these topics before you get started:

Jira Cloud SSO Requirements

Before you configure the Jira Cloud web application for SSO, you need the following:

- A Jira Cloud account.
- An organization administrator and Jira Cloud site administrator (user with admin permission in the group “site-admins”)
- Domains of SSO users’ email addresses added and verified before configuration.

Configuring Your Organizations

Atlassian uses organizations to manage your domains and user accounts, providing control and visibility across your Atlassian Cloud applications. Setting up your organization and verifying a domain are pre-requisites to configuring SSO. Refer to https://confluence.atlassian.com/cloud/organization-administration-938859734.html for more information about configuring your organization with Atlassian.

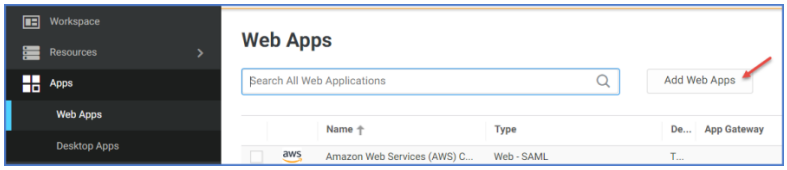
Adding and Configuring Jira Cloud in Admin Portal

The following steps are specific to the Jira Cloud application and are required in order to enable SSO for Jira Cloud. For information on optional configuration settings available in the Delinea Admin Portal, see "Optional Configuration Settings" on page 844.

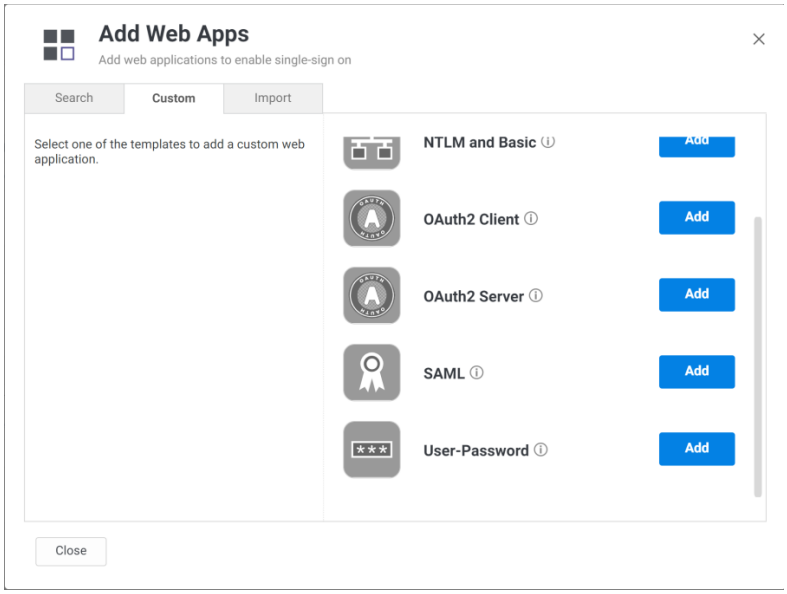
To add and configure the Jira Cloud application in the Admin Portal:

1. In the Admin Portal, select **Apps > Web Apps**, then click **Add Web Apps**.

   The Add Web Apps screen appears.

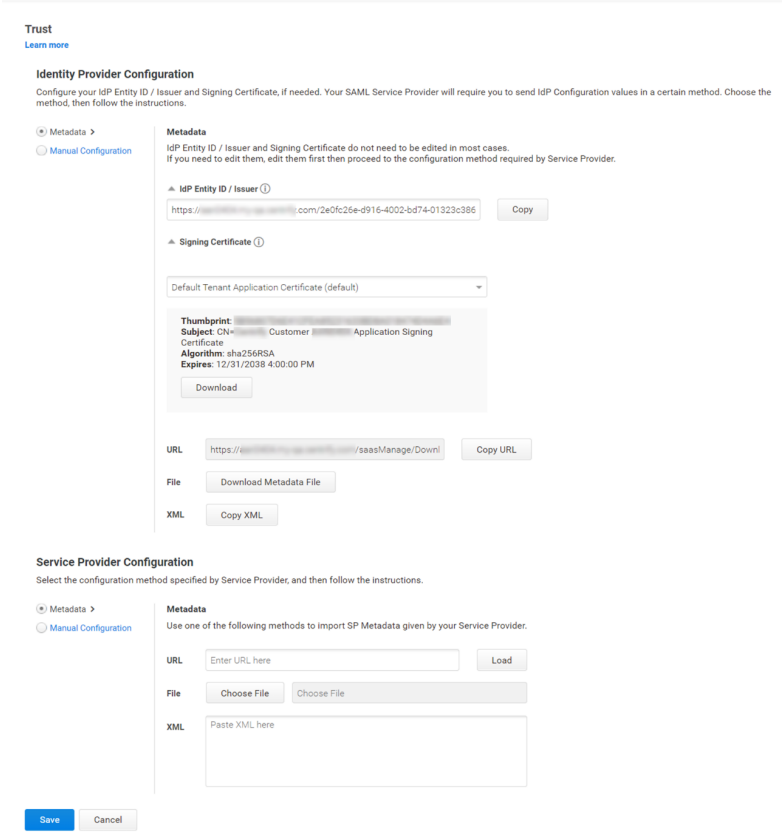


2. On the Search tab, enter the partial or full application name in the **Search** field and click the search icon.

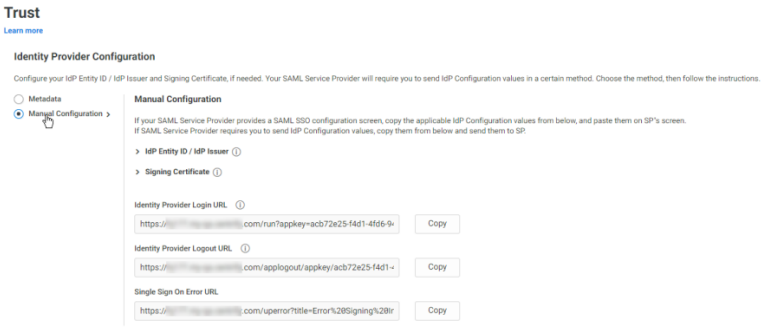


3. Next to the application, click **Add**.
4. In the Add Web App screen, click **Yes** to confirm.
5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Settings page.
6. Click the **Trust** page to begin configuring the application.



The UI is evolving in order to simplify application configuration. For example, many of the settings previously found on the Application Settings page are now on the Trust page. You might have to select **Manual Configuration** to expose those settings, as shown in the following example.



Any previously configured applications retain their configuration and do not require reconfiguration. If you are configuring an application for the first time, refer to the Trust page for any settings previously found on the Application Settings page.

In addition, the description of how to choose and download a signing certificate in this document might differ slightly from your experience. See "Choose a Certificate File" on page 842 for the latest information.

Configuring Jira Cloud for SSO

You need organization administrator privileges to perform these steps.

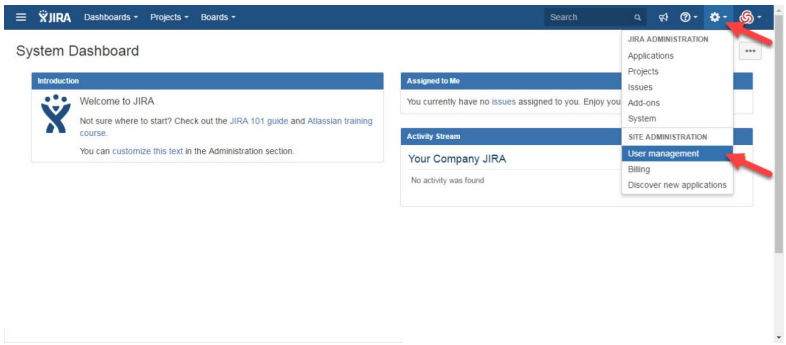
Tip: It can be useful to open the web application and Admin Portal simultaneously and have them both open, perhaps side by side. As part of the SSO configuration process, you'll need to copy and paste settings between the two browser windows.

The following steps are specific to the Jira Cloud application and are required in order to enable SSO for Jira Cloud. For information on optional configuration settings available in the Delinea Admin Portal, see "Optional Configuration Settings" on page 844.

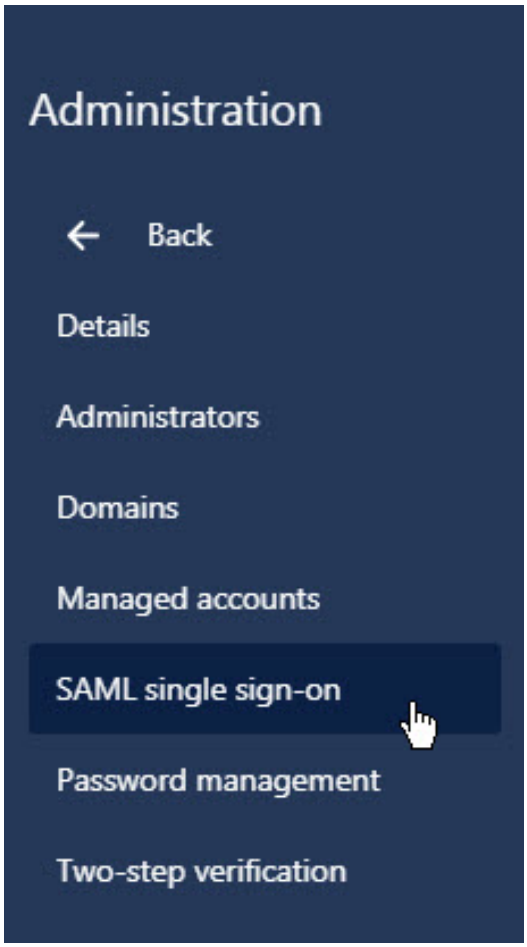
To configure Jira Cloud for SSO:

1. Return to the browser tab where you added and verified email addresses. If that browser tab is no longer active, open a new browser tab and log in to Jira Cloud with an account that has ADMIN privileges in the group "site-admins" and is an organization administrator.

   Click **Settings** > **User management**, then navigate to **Organizations & Security** and select your verified domain.



2. Click **SAML single sign-on**.



3. On the Atlassian SAML single sign-on page, click **Add SAML configuration**.
4. On the Add SAML configuration screen, configure the following:

Admin Portal >Application Settings	Copy/Paste Direction	Jira Cloud Website >Atlassian Site Administration	What you do
Identity Provider Entity ID	-->	Identity Provider Entity ID	Copy the URL from the Admin Portal and paste here.
Identity Provider SSO URL	-->	Identity Provider SSO URL	Copy the URL from the Admin Portal and paste here.
Download Signing Certificate	-->	Public x509 Certificate	Click Download Signing Certificate in the Admin Portal and open the file in a text editor. Copy the contents and paste it here.

5. Click **Save configuration**.
6. Compare the following settings between the Atlassian SAML single sign-on page and the Application Settings page of the Delinea Admin Portal.

   The red arrows in the table below indicate the direction of the copy and paste operation between the two windows. For instance, the first arrow in the table below indicates that you copy the content from the indicated field on the Jira Cloud website and paste it into the corresponding field in the Privileged Access Service Admin Portal.

Admin Portal >Application Settings	Copy/Paste Direction	Jira Cloud Website >Atlassian Site Administration	What you do
SP Entity ID	<--	SP Entity ID	If the SP Entity ID is not: https://id.atlassian.com/login, copy the SP Entity ID from Jira Cloud and paste it in the Admin Portal Application Settings page.
SP Assertion Consumer Service URL	<--	SP Assertion Consumer Service URL	If your SP Assertion Consumer Service URL is not: https://id.atlassian.com/login/saml/acs, copy the SP Assertion Consumer Service URL from Jira Cloud and paste it in the Admin Portal Application Settings page.

7. In the Privileged Access Service Admin Portal, configure User Access and Account Mapping.
8. Click **Save**.

Configuring Jira Cloud Mobile Apps for SSO

Jira Cloud provides mobile applications that support SSO for iOS and Android devices.

SP-initiated SSO will be launched after you enter the site name (subdomain) of your Jira Cloud and an email address with a verified domain.

For more information about Jira Cloud

See "Configuring Jira Cloud for SSO" on page 897 for more information.

Jira Cloud Specifications

Each SAML application is different. The following table lists features and functionality specific to Jira Cloud.

Capability	Supported?	Support details
Web browser client	Yes	
Mobile client	Yes	iOS and Android

Capability	Supported?	Support details
SAML 2.0	Yes	
SP-initiated SSO	Yes	
IdP-initiated SSO	Yes	
Force user login via SSO only	Yes	Users with an email address at a domain that has been verified must use SSO.
Separate administrator login after SSO is enabled	No	
User or Administrator lockout risk	Yes	
Automatic user provisioning	No	
Multiple User Types	Yes	SSO works the same way for all admin and non-admin user types.
Self-service password	Yes	Users can reset their own passwords. Resetting another user's password requires administrator rights.
Access restriction using a corporate IP range	Yes	You can specify an IP Range in the Admin Portal Policy page to restrict access to the application.

JIRA Server (On-Premise)

With Delinea as your Privileged Access Service, you can configure JIRA Server (On-Premise) for either or both IdP-initiated SAML SSO and SP-initiated SAML SSO (for SSO access directly through the JIRA Server web application). Enabling both methods ensures that users can log in to JIRA Server in different situations such as clicking through a notification email.

Note: After you configure SAML SSO, JIRA username-password login pages will not function. It will display a login error even if the correct username and password are entered.

JIRA does not support SAML, but it accepts a custom plugin for individual companies to modify the authentication process to their own needs, including implement Single Sign-On. A custom plugin is a set of .jar files that are implemented using Atlassian's Seraph library, and will be deployed in the JIRA Server. A system administrator must change the JIRA configuration to use the plugin.

With Delinea JIRA SAML plugin deployed in JIRA Server, any unauthenticated access to JIRA resources will be redirected to Delinea Admin Portal for authentication. After that, users will be redirected back to the requested resources.

Delinea JIRA SAML plugin supports JIRA Server versions 6.x and 7.x.

If JIRA is the first application you are configuring for SSO through Privileged Access Service, read these topics before you get started:

- "Introduction to Application Management" on page 823
-

JIRA Server SSO requirements

Before you configure the JIRA Server web application for SSO, you need the following:

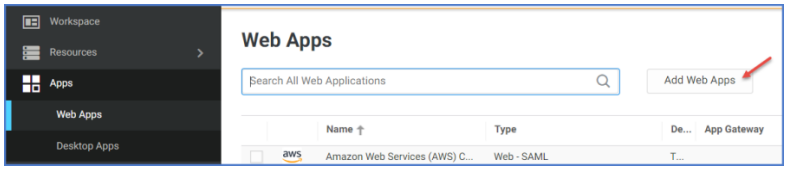
- A JIRA Server (On-Premise).
- A system administrator account to the JIRA Server computer to deploy and configure the plugin.

Configuring JIRA Server in Admin Portal

The following steps are specific to the JIRA application and are required in order to enable SSO for JIRA. For information on optional configuration settings available in the Delinea Admin Portal, see "Optional Configuration Settings" on page 844.

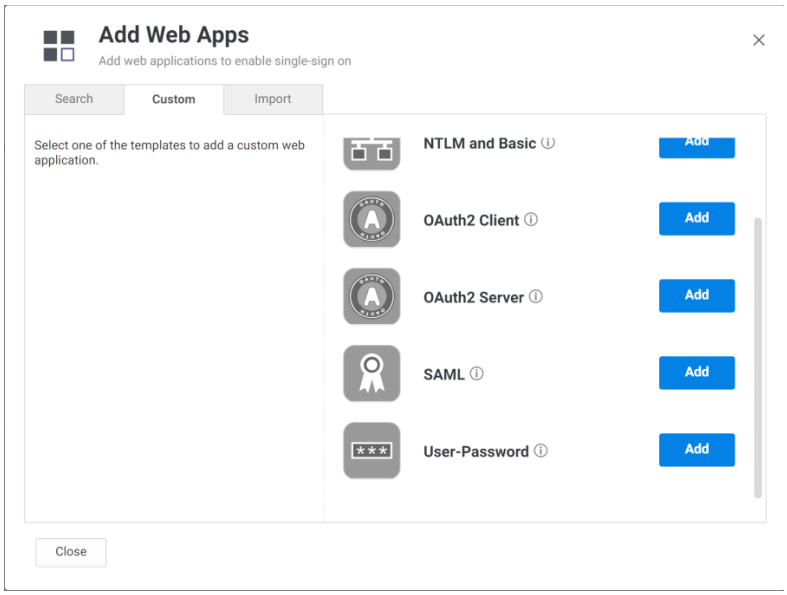
To add and configure the JIRA Server application in Admin Portal:

1. In Admin Portal, click **Apps**, then click **Add Web Apps**.



   The Add Web Apps screen appears.

2. On the Search tab, enter the partial or full application name in the Search field and click the search icon.

3. 

4. Next to the application, click **Add**.
5. In the Add Web App screen, click **Yes** to confirm.

   Admin Portal adds the application.
6. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Application Settings page.

   Note: The description of how to choose and download a signing certificate in this document might differ slightly from your experience. See "Choose a Certificate File" for the latest information.
7. Configure the following:

Field	Set it to	What you do
Assertion Consumer Service URL	Your JIRA Server host and port number.	

8. Click **Account Mapping** in the Admin Portal and see "Map User Accounts" on page 840 for configuration details.

   Note: If your JIRA Server is hosted over HTTP, change https to http. |
9. In **Account Mapping**:
   a. Select **Use the following Directory Service field to supply the user name**.
   b. In **Directory Service field name**, replace *userprincipalname* with your company's Active Directory field name that stores the JIRA Employee ID.
   c. Click **Save**.

      Note: For information on optional Delinea Admin Portal configuration settings that you may wish to customize for your app, see "Optional Configuration Settings" on page 844.

Downloading the Delinea JIRA SAML Plugin and Signing Certificate

To download the plugin and certificate:

1. Go to the **Application Settings** page for the JIRA Server app in Admin Portal.
2. Copy your **IdP Issuer** and save it where you can find it in the next step.
3. Copy your **IdP Post URL** and save it where you can find it in the next step.
4. Click **Download Signing Certificate** and save the .cer file where you can find it in the next step.
5. Click **Download this plugin to be installed into your JIRA Server instance** to download a .zip file containing the SAML plugin files, and save the file where you can find it in the next step.

Deploying and Configuring JIRA SAML Plugin in JIRA Server

This section requires a system administrator to place new files in the JIRA Server file system and modify JIRA configuration files. Note that this is a system administrator to the server hosting JIRA, not a JIRA (application) administrator.

Note: These instructions assume:

- JIRA on Windows.
- JIRA installed as a Windows Service.

To deploy and configure the JIRA SAML plugin:

1. Access the server hosting JIRA.
2. Stop the JIRA application. For example, in Windows 7, go to **Control Panel > Administrative Tools > Services**, then right-click **Atlassian JIRA** the service and select **Stop**.
3. Copy the .cer signing certificate file downloaded in the previous steps and place it in:

   <your-atlassian-directory>\JIRA.
4. Copy the .zip file downloaded in the previous steps and place it in a temporary location (any location other than where it will be moved to in the next few steps).
5. Extract the .zip file. The extracted contents are:
   - File: readme.txt
   - Directory: atlassian-jira
   - Directory: conf
6. Copy all the .jar files from the directory atlassian-jira\WEB-INF\lib and paste them in your JIRA directory at:

   <your-atlassian-directory>\JIRA\atlassian-jira\WEB-INF\lib
7. Go to *<your-atlassian-directory>*\JIRA\atlassian-jira\WEB-INF\lib.

   You will see there are two files named xmlsec-*<x.x.x>*.jar.
8. If your JIRA is version 6.1 or later, delete xmlsec-1.4.5.jar. Otherwise, delete xmlsec-1.1.0.jar.
9. Go to *<your-atlassian-directory>*\JIRA\lib.

10. Copy the following .jar files and paste them in *<your-atlassian-directory>*\JIRA\atlassian-jira\WEB-INF\lib:
    - jcl-over-slf4j-x.x.x.jar
    - slf4j-api-x.x.x.jar
    - slf4j-log4j12-x.x.x.jar
11. Copy the atlassian-jira\WEB-INF\classes directory and paste it in your JIRA directory at *<your-atlassian-directory>*\JIRA\atlassian-jira\WEB-INF\classes.

    This will place two custom email template files in your JIRA directory:
    - *<your-atlassian-directory>*\JIRA\atlassian-jira\WEB-INF\classes\templates\email\html\centrify-usercreated-nopassword.vm
    - *<your-atlassian-directory>*\JIRA\atlassian-jira\WEB-INF\classes\templates\email\text\centrify-usercreated-nopassword.vm
12. Copy the catalina-saml.properties file in the conf directory, and paste it in your JIRA directory: *<your-atlassian-directory>*\JIRA\conf.
13. Use your favorite text editor to open *<your-atlassian-directory>*\JIRA\atlassian-jira\WEB-INF\classes\seraph-config.xml.
14. Find the following authenticator lines and comment out the one that is being used:

    <authenticator class="com.atlassian.jira.security.login.JiraSeraphAuthenticator"/>

    <authenticator class="com.atlassian.jira.security.login.SSOSeraphAuthenticator"/>.
15. Add this new authenticator line to seraph-config.xml:

    <authenticator class="com.centrify.cloud.saas.jirasaml.SamlAuthenticator"/>
16. Save seraph-config.xml.
17. Open *<your-atlassian-directory>*\JIRA\atlassian-jira\WEB-INF\web.xml.
18. Find the last <servlet> defined.
19. Place your cursor **below** the last <servlet> defined, then copy/paste the following:

    <!-- Centrify JIRA SAML -->

    <servlet>

    <servlet-name>samlServlet</servlet-name>

    <servlet-class>com.centrify.cloud.saas.jirasaml.SamlServlet</servlet-class>

    <init-param>

    <param-name>defaultHomepage</param-name>

    <!-- If you want SAML Users to land on a specific page, enter the URI after https://(jira-host)/ without

    a slash in the front. For example, if you want SAML Users to land on the Issues page,

    https://(jira-host)/issues, enter "issues" here as the param-value.

    Leaving an empty string will bring a SAML User to the user's My JIRA Home page. -->

<param-value></param-value>

</init-param>

<init-param>

<param-name>idpIssuerName</param-name>

<param-value><!-- Copy IdP Issuer from Application Settings in Centrify and paste it here. --></param-value>

</init-param>

<init-param>

<param-name>idpCertFile</param-name>

<param-value><!-- Absolute file path to your signing certificate file --></param-value>

</init-param>

<init-param>

<param-name>audience</param-name>

<!-- After setting the audience value below, make sure you also set the same audience value in Admin Portal. --
>

<param-value>JIRA</param-value>

</init-param>

<load-on-startup>1</load-on-startup>

</servlet>

20. Set the <param-value> of idpCertFile to the absolute file path to your signing certificate file. If you used the recommended path name in Step 3 and if your certificate file is named JIRA.cer, you would set <param-value> to:

    <your-atlassian-directory>\JIRA\JIRA.cer.

    As shown here:

    <init-param>

    <param-name>idpCertFile</param-name>

    <param-value>C:\Program Files\Atlassian\JIRA\JIRA.cer<param-value>

    </init-param>

21. Find the last <servlet-mapping> defined.
22. Place your cursor **below** the last <servlet-mapping> and copy/paste the following:

    <!-- Centrify JIRA SAML -->

    <servlet-mapping>

    <servlet-name>samlServlet</servlet-name>

    <url-pattern>/saml</url-pattern>

    </servlet-mapping>

23. Save web.xml.
24. Open *<your-atlassian-directory>*\Atlassian\JIRA\conf\catalina-saml.properties in a text editor.
25. Open the catalina.properties file of your JIRA in a text editor. By default, the file is located at: *<your-atlassian-directory>*\JIRA\atlassian-jira\conf\.
26. Copy the contents of the catalina-saml.properties file and paste them at the end of your catalina.properties file.
27. Save catalina.properties.
28. Start the JIRA application. For example, in Windows 7, go to **Control Panel > Administrative Tools > Services**, then right-click **Atlassian** JIRA the service and select **Start**.

    Wait a few minutes for the service to start. The new settings that you just configured will be used after JIRA starts.
29. Test and verify that your newly installed IdP-initiated SSO to JIRA works properly before proceeding.

    Now that you have finished configuring the application settings in the Admin Portal and the JIRA application, users are ready to launch the application from the Admin Portal.

    Note: There are several optional configuration steps available:

- "(Optional) Configuring SP-initiated SSO for JIRA Server" below.
- "(Optional) Closing the Back Door Login for SP-Initiated SSO for JIRA Server" on page 908.
- "(Optional) Disabling Just-In-Time User Provisioning" on page 909.
- "(Optional) Disabling SAML User Update" on page 909.
- "(Optional) Disabling SAML group update" on page 910.

(Optional) Configuring SP-initiated SSO for JIRA Server

If you also want to use SP-initiated SSO, complete the steps in this section.

Note: After you configure SP-initiated SSO, JIRA username-password login pages will not function. For more information about what this means and what your options are with SP-initiated SSO, see "(Optional) Closing the Back Door Login for SP-Initiated SSO for JIRA Server" on page 908.

To configure SP-initiated SSO:

1. Stop the JIRA application. For example, in Windows 7, go to **Control Panel > Administrative Tools > Services**, then right-click **Atlassian JIRA** the service and select **Stop**.
2. In your favorite text editor, open *<your-atlassian-directory>*\JIRA\atlassian-jira\WEB-INF\web.xml.
3. Find the <filter> with the name JiraLastFilter.
4. Place your cursor **above** this <filter>, and copy/paste the following:

   <!-- Centrify JIRA SAML -->

   <filter>

   <filter-name>samlFilter</filter-name>

   <filter-class>com.centrify.cloud.saas.jirasaml.SamlFilter</filter-class>

<init-param> <!-- Required -->

<param-name>idpPostUrl</param-name>

<param-value></param-value>

</init-param>

<init-param> <!-- Required -->

<param-name>spIssuerName</param-name>

<param-value>JIRA</param-value>

</init-param>

<init-param> <!-- Required -->

<param-name>allowedURIs</param-name>

<param-value>

/saml,

/plugins/servlet/applinks/*,

/plugins/servlet/oauth/*,

/rest/*

</param-value>

</init-param>

</filter>

5. Set the <param-value> of idpPostUrl to the **IdP Post URL** that you copied from your JIRA Server SAML application in the previous steps.
6. Set the <param-value> of idpIssuerName to the **IdP Issuer** that you copied from your JIRA Server SAML application in the previous steps.
7. Find the <filter-mapping> with the name login.
8. Place your cursor **below** this <filter-mapping>, and copy/paste the following:

   <!-- Centrify JIRA SAML -->

   <filter-mapping>

   <filter-name>samlFilter</filter-name>

   <url-pattern>/*</url-pattern>

   </filter-mapping>
9. Save web.xml.
10. Start the JIRA application. For example, in Windows 7, go to **Control Panel > Administrative Tools > Services**, then right-click **Atlassian JIRA** the service and select **Start**.

    Wait a few minutes for the service to start. The new settings that you just configured will be used after JIRA starts.

Note: After configuration for SP-initiated SSO is complete, the JIRA application is automatically ready to link to other Atlassian apps released in that have also been configured for SP-initiated SSO. For information about how to link the apps, see:

Note: You can add additional paths to the list of <param-value> values for allowedURIs in the web.xml file for Atlassian apps released in Privileged Access Service Cloud 17.10 or later. It is important that you do not change the /saml <param-value>.

(Optional) Closing the Back Door Login for SP-Initiated SSO for JIRA Server

If you configure SP-initiated SSO, JIRA login pages are disabled and users run the risk of being locked out of JIRA. The only way that users can sign back in with their JIRA username and password after they have been locked out is to append the parameters os_username and os_password to the end of their JIRA URL, with the URL-encoded username and password values. For example if your username is jsmith@acme.com and the password is NoPwd!, your URL would be:

https://jira.acme.com/?os_username=jsmith%40acme.com&os_password=NoPwd!

This is not secure because the password is exposed, but is the only way to use JIRA username and password to log in after SP-initiated SSO is configured. If your company wants to have SP-initiated SSO and to disable JIRA's query parameter authentication, follow the steps below.

To disable back door login for SP-initiated SSO:

1. Stop the JIRA application. For example, in Windows 7, go to **Control Panel > Administrative Tools > Services**, then right-click **Atlassian JIRA** the service and select **Stop**.
2. In your favorite text editor, open *<your-atlassian-directory>*\JIRA\atlassian-jira\WEB-INF\web.xml.
3. Find the <filter-mapping> with the name samlFilter.
4. Move the whole <filter-mapping> with the name samlFilter **before** the <filter-mapping> with the name login. For example:

   <!-- Centrify JIRA SAML -->

   <filter-mapping>

   <filter-name>samlFilter</filter-name>

   <url-pattern/*</url-pattern>

   </filter-mapping>

   <filter-mapping>

   <filter-name>login</filter-name>

   <url-pattern/*</url-pattern>

   <dispatcher>REQUEST</dispatcher>

   <dispatcher>FORWARD</dispatcher>

   </filter-mapping>
5. Save web.xml.

6. Start the JIRA application. For example, in Windows 7, go to **Control Panel > Administrative Tools > Services**, then right-click **Atlassian JIRA** the service and select **Start**.

   Wait a few minutes for the service to start. The new settings that you just configured will be used after JIRA starts.

   Note: Please note that the os_username and os_password parameters can still be used while calling JIRA RESTful services. For example if your username is jsmith@acme.com and the password is NoPwd!, your URL would be:

   https://jira.acme.com/rest/api/latest/issue/PC-11?os_username=jsmith%40acme.com&os_password=NoPwd!

(Optional) Disabling Just-In-Time User Provisioning

The setting to enable or disable just-in-time user provisioning is located in your JIRA catalina.properties file, by default located in *<your-atlassian-directory>*\conf*.*

To disable just-in-time user provisioning:

1. Open *<your-atlassian-directory>*\conf\catalina.properties in a text editor.
2. Find com.centrify.cloud.saas.jirasaml.jitUserProv.enabled.
3. Set its value to false.
4. Save catalina.properties.
5. Start the JIRA application. For example, in Windows 7, go to **Control Panel > Administrative Tools > Services**, then right-click **Atlassian JIRA** the service and select **Start**.

   Wait a few minutes for the service to start. The new settings that you just configured will be used after JIRA starts.

To disable only the email notification of just-in-time user provisioning:

1. Open *<your-atlassian-directory>*\conf\catalina.properties in a text editor.
2. Find com.centrify.cloud.saas.jirasaml.jitUserProv.sendsEmail.
3. Set its value to false.
4. Save catalina.properties.
5. Start the JIRA application. For example, in Windows 7, go to **Control Panel > Administrative Tools > Services**, then right-click **Atlassian JIRA** the service and select **Start**.

   Wait a few minutes for the service to start. The new settings that you just configured will be used after JIRA starts.

(Optional) Disabling SAML User Update

SAML user update will update a JIRA user's email address and full name to the ones specified in SAML assertion. The setting to enable or disable this feature is located in your JIRA catalina.properties file, by default located in *<your-atlassian-directory>*\conf*.*

To disable user update:

1. Open *<your-atlassian-directory>*\conf\catalina.properties in a text editor.
2. Find com.centrify.cloud.saas.jirasaml.samlUserUpdate.enabled.
3. Set its value to false.
4. Save catalina.properties.
5. Start the JIRA application. For example, in Windows 7, go to **Control Panel > Administrative Tools > Services**, then right-click **Atlassian JIRA** the service and select **Start**.

Wait a few minutes for the service to start. The new settings that you just configured will be used after JIRA starts.

(Optional) Disabling SAML group update

SAML group update will update a JIRA user's groups in JIRA to the ones specified in SAML assertion. The setting to enable or disable this feature is located in your JIRA catalina.properties file, by default located in *<your-atlassian-directory>*\conf*.*

To disable group update:

1. Open *<your-atlassian-directory>*\conf\catalina.properties in a text editor.
2. Find com.centrify.cloud.saas.jirasaml.samlGroupUpdate.enabled.
3. Set its value to false.
4. Save catalina.properties.
5. Start the JIRA application. For example, in Windows 7, go to **Control Panel > Administrative Tools > Services**, then right-click **Atlassian JIRA** the service and select **Start**.

   Wait a few minutes for the service to start. The new settings that you just configured will be used after JIRA starts.

For More Information

- See "JIRA Server specifications" below for a list of features and functionality specific to JIRA.
- For JIRA non-SSO information, see JIRA Documentation.
- For configuration between Delinea SAML Plug-in and JIRA Server, contact Delinea Support.

JIRA Server specifications

Each SAML application is different. The following table lists features and functionality specific to JIRA Server.

Capability	Supported?	Support details
Web browser client	Yes	
Mobile client	No	
SAML 2.0	Yes	

Capability	Supported?	Support details
SP-initiated SSO	Yes, optional	
IdP-initiated SSO	Yes	
Force user login via SSO only	Yes	
Separate administrator login after SSO is enabled	No	
User or Administrator lockout risk	Yes	Because SP-initiated SSO always redirects users to Delinea and disables the function of JIRA login pages, users run the risk of being locked out of JIRA. The configuration in leaves JIRA's query parameter authentication available, so that users can use their JIRA username and password to log in to JIRA if needed. For more information about using JIRA's query parameter authentication to set up a back door URL for administrators and users, see .
Automatic user provisioning	Yes	
Multiple User Types	Yes	SSO works the same way for all admin and non-admin user types.
Self-service password	Yes	Users can reset their own passwords. Resetting another user's password requires administrator rights.
Access restriction using a corporate IP range	Yes	You can specify an IP Range in the Admin Portal Policy page to restrict access to the application.

Palo Alto Networks

With Delinea as your Privileged Access Service, you can choose single-sign-on (SSO) access to the Palo Alto Networks web applications with SP-initiated SAML SSO for SSO access directly through the Palo Alto Networks web application.

If Palo Alto Networks is the first application you are configuring for SSO through Privileged Access Service, read these topics before you get started:

- "Introduction to Application Management" on page 823

Continue with "Palo Alto Networks SSO Requirements" on the next page

Palo Alto Networks SSO Requirements

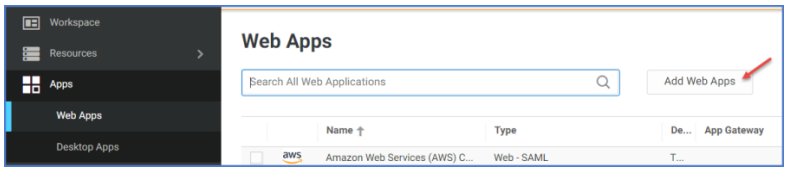
Before you can configure Palo Alto Networks for SSO, you need the following:

- An active Palo Alto Networks account that has account administrator rights for your organization.

Adding and Configuring Palo Alto Networks in the Admin Portal

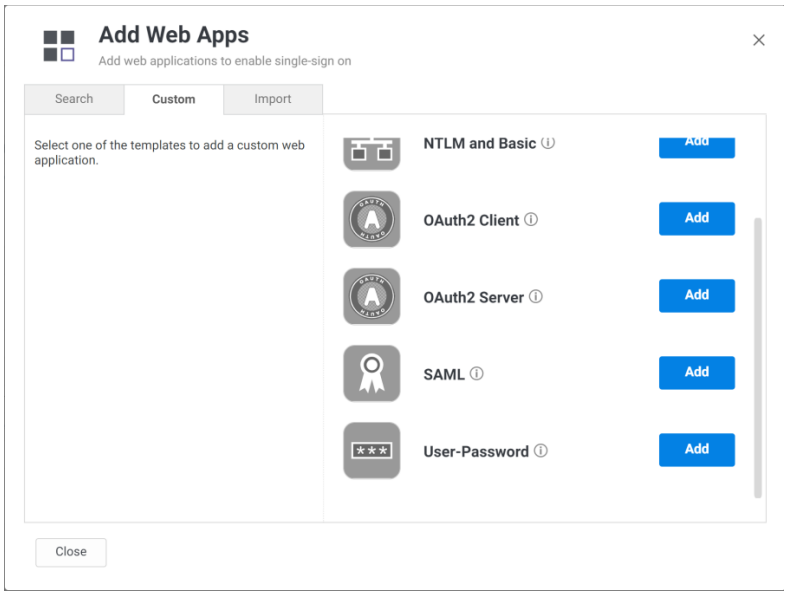
To add and configure Palo Alto Networks in the Admin Portal:

1. In Admin Portal, click **Apps**, then click **Add Web Apps**.



   The Add Web Apps screen appears.

2. On the Search tab, enter the partial or full application name in the Search field and click the search icon.



3. Next to the application, click **Add**.
4. In the Add Web App screen, click **Yes** to confirm.

   Admin Portal adds the application.

5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Application Settings page.

> **Note:** The description of how to choose and download a signing certificate in this document might differ slightly from your experience. See "Choose a Certificate File" on page 842 for the latest information.

6. If you want to use a different security certificate, set it under Additional Options.

   See "Choose a Certificate File" on page 842 for more information.

7. Click **Download Identity Provider Metadata** and save it on your computer.

   You will need this file when "Configuring SSO for Palo Alto Networks" below.

8. Keep this browser window open for use later in the configuration process.

Configuring SSO for Palo Alto Networks

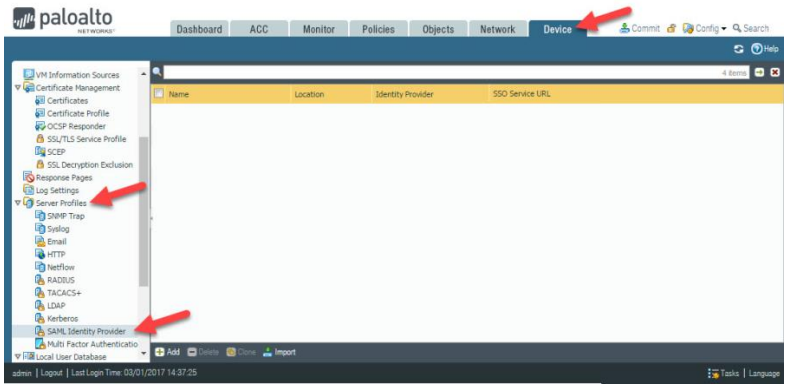
The following steps are specific to the Palo Alto Networks application and are required in order to enable SSO for Palo Alto Networks. For information on optional Delinea Admin Portal configuration settings that you may wish to customize for your app, see "Optional Configuration Settings" on page 844.

To configure Palo Alto Networks for SSO:

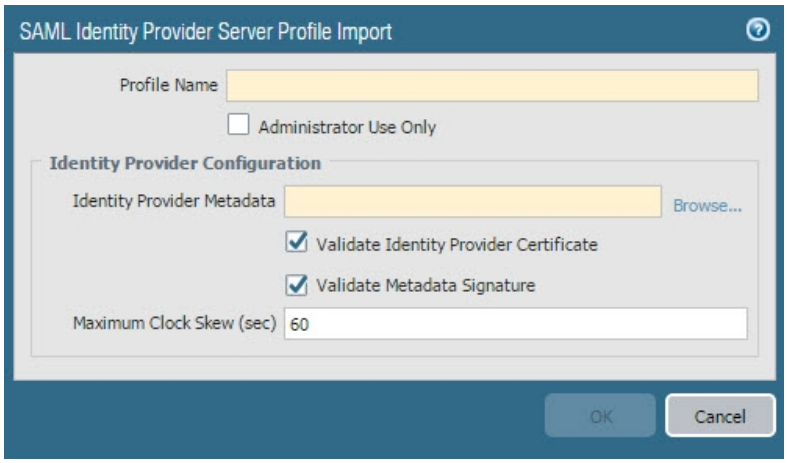
1. Open a new tab in your web browser.

   Note: It is helpful to open the Palo Alto Networks web application and the Delinea Admin Portal Application Settings window simultaneously to copy and paste settings between the two browser windows.

2. In your web browser, sign in to Palo Alto Networks as Admin.
3. Click on the **Device** tab and select **Server Profiles > SAML Identity Provider** from the menu on the left side of the page.

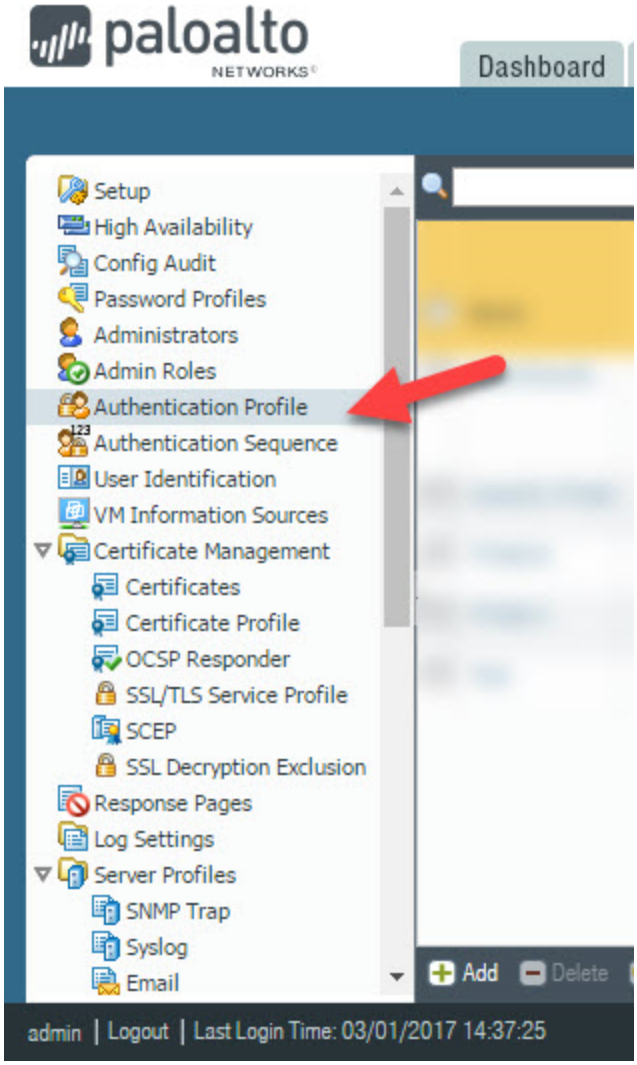


4. Click **Import** at the bottom of the page.

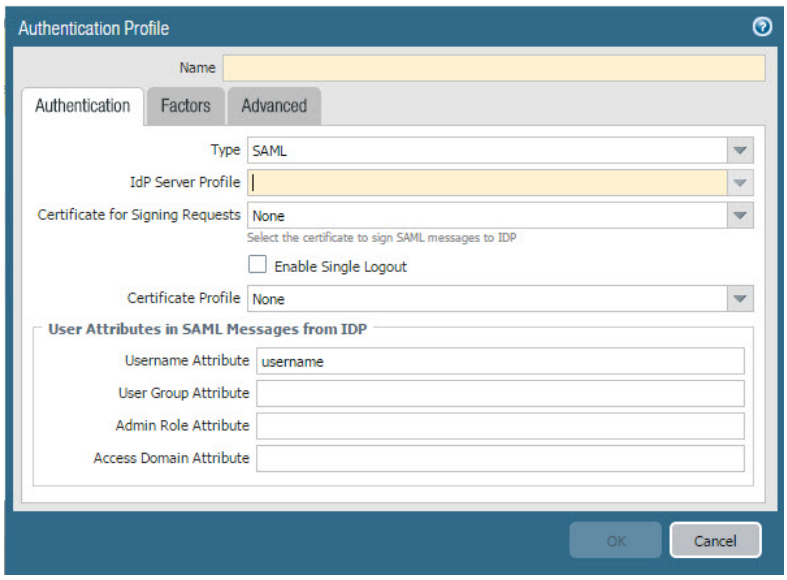


5. Enter a **Profile Name**.
6. (Optional) Select **Administrator Use Only** if you want only administrators to use SAML SSO.
7. For Identity Provider Metadata, click **Browse...**
8. Select the **Identity Provider Metadata** file that you downloaded in "Adding and Configuring Palo Alto Networks in the Admin Portal" on page 912.
9. Palo Alto Networks recommends that you use a CA certificate. If you have one, select **Validate Identity Provider Certificate** and then refer to Palo Alto Networks documentation to add the certificate and create a Certificate Profile.

   Note: While a less secure method, if you do not have a certificate from a trusted Certificate Authority (CA), unselect **Validate Identity Provider Certificate**. The default Signing Certificate provided by Privileged Access Service Admin Portal is a self-signed certificate, and not a trusted CA certificate.
10. Select **Validate Metadata Signature**.
11. In most cases you can leave **Maximum Clock Skew (sec)** set to the default value, but you can configure the clock skew for your app to whatever you like. The maximum value is the allowed difference in seconds between the system times of the IdP and the firewall at the moment when the firewall validates IdP messages (default is 60; range is 1 to 900). If the difference exceeds this value, authentication fails.
12. Click **OK**.
13. Select the server profile that you just created.
14. On the **Device** tab, select **Authentication Profile** from the menu on the left side of the page.



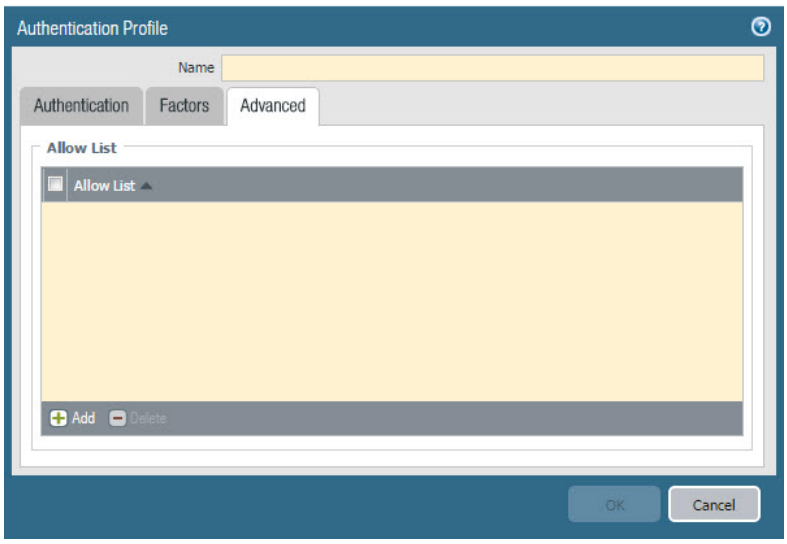
15. Click **Add** at the bottom of the page.



16. Enter a **Name** for your profile.
17. Select **SAML** from the **Type** drop-down list.
18. In the **IdP Server Profile** drop-down list, select the name of the server profile you just created.
19. Leave **Certificate for Signing Requests** set to **None**.
20. (Optional) Select **Enable Single Logout** if you want users to also log out from Privileged Access Service when they sign out of the Palo Alto Networks app.
21. If you previously selected **Validate Identity Provider Certificate** when you configured your profile, select your profile in the **Certificate Profile** field.

    Note: Leave all the attribute values with their default values.

22. Click on the **Advanced** tab in the Authentication Profile window.



23. Add the user, groups, and roles that will use SAML SSO.
24. Click **OK**.
25. Click the **Metadata** link in the Authentication column for your profile to download the Service Provider Metadata file that you will need to upload to the Delinea Admin Portal.
26. Configure Palo Alto Networks features to use the Authentication Profile you just created.

    Note: Many of the other features you can configure on the Palo Alto Networks configuration page will ask you to choose an Authentication Profile from the drop-down box. When you see this option, you will always need to choose the profile you created. After you configure each feature you will need to click **OK** and then click **Commit**.

    Note: After an Authentication Profile is created for an Administrator, they are no longer able to sign in with their username and password.
27. Return to the browser window you have open to the Application Settings page in the Delinea Admin Portal.
28. Click the **Upload SP Metadata** button.
29. Select **Upload SP Metadata from a file** and click **Browse**.
30. Select the Service Provider Metadata file you downloaded from Palo Alto Networks above.
31. Click **OK**.

For more information about Palo Alto Networks

Palo Alto Networks Support:

https://live.paloaltonetworks.com/t5/custom/page/page-id/Support

Palo Alto Networks Specifications

Each SAML application is different. The following table lists features and functionality specific to Palo Alto Networks.

Capability	Supported?	Support details
Web browser client	No	
Mobile client	No	
SAML 2.0	Yes	
SP-initiated SSO	Yes	
IdP-initiated SSO	No	
Force user login via SSO only	Yes	After a user is configured to use SSO, they can only use SSO.
Separate administrator login after SSO is enabled	No	We recommend that you always keep one admin user who does not use SSO.
User or Administrator lockout risk	Yes	We recommend that you always keep one admin user who does not use SSO.
Automatic user provisioning	No	
Multiple User Types	Yes	Admin and User.
Self-service password	Yes	
Access restriction using a corporate IP range	Yes	You can specify an IP Range in the Admin Portal Policy page to restrict access to the application.

Splunk

Splunk offers both IdP-initiated SAML SSO (for SSO access through the Admin Portal) and SP-initiated SAML SSO (for SSO access directly through the Splunk web application). You can configure Splunk for either or both types of SSO.

Note: This document is written for Splunk On-Premise 8.x. If you are not using this version, your interface may differ from the descriptions in this document.

Splunk SSO Requirements

Before you configure the Splunk web application for SSO, you need the following:

- A registered Privileged Access Service account and at least one Delinea Connector installed on a Windows computer (if you use only the Privileged Access Service directory as your identity store, you do not need to install the Delinea Connector).
- A running version of Splunk Enterprise.
- An active Splunk Enterprise account with administrator rights for your organization.

- Delinea or your Active Directory configured to provide the role, realName, and mail attributes for the SSO user.
- An admin role with change authentication capability. This permission level lets you enable SAML and edit authentication settings on the Splunk search head.
- A signed certificate in both the Splunk web application and Delinea Admin Portal. You can either download one from Admin Portal or use your organization's trusted certificate. If you use your own certificate, upload the signing certificate and its private key in a .pfx or .p12 file to the application settings in Admin Portal, and upload the public key certificate in a .cer or .pem file to the web application.

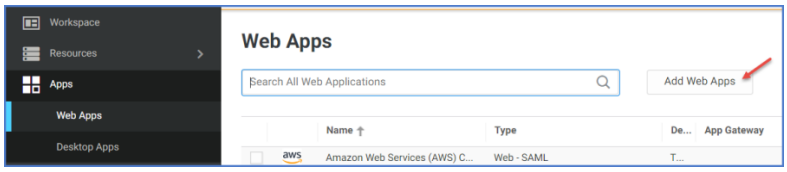
  Note: Currently Splunk does not support certificate chaining and the certificate provided to Splunk must be publicly verifiable.

- The Privileged Access Service tenant certificate contains two certificates in chain. If you use the Privileged Access Service tenant certificate for your application and you provide that certificate to Splunk, the application will fail to validate the SAML response. If you use that certificate for your application, you must provide the Delinea CA certificate (the root certificate from the Delinea tenant certificate in Splunk) for the Splunk application to correctly verify the signature.
- If you have more than two certificates in chain, e.g. **Leaf > Intermediate > Root** and you provide the **Leaf** certificate to Splunk, Splunk will fail to validate the SAML response. In this case you must follow the steps explained in this Splunk forum answer:

Adding the Splunk App in Admin Portal

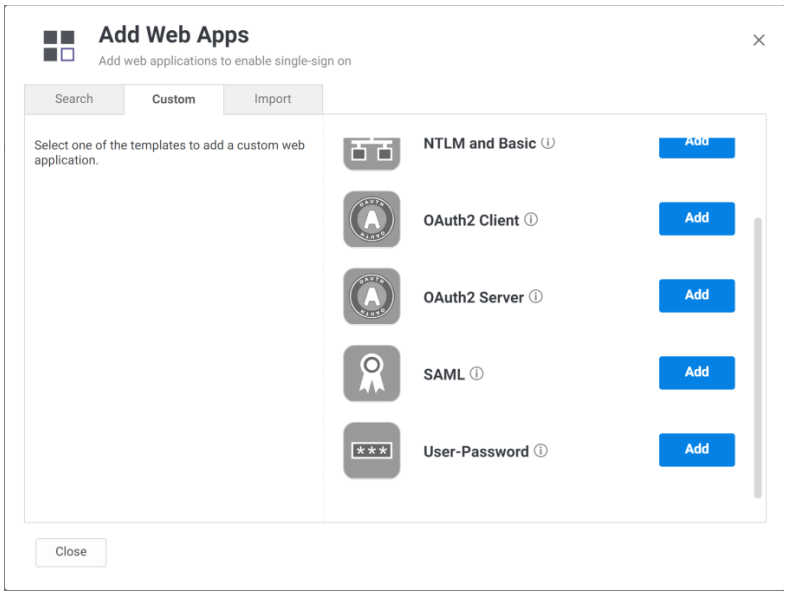
To add the Splunk application in Admin Portal:

1. In the Admin Portal, click **Apps**, then click **Add Web Apps**.



   The Add Web Apps screen appears.

2. On the Search tab, enter the partial or full application name in the Search field and click the search icon.



3. Next to the application, click **Add**.
4. In the Add Web App screen, click **Yes** to confirm.

   Admin Portal adds the application.
5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Application Settings page.

> **Note:** The description of how to choose and download a signing certificate in this document might differ slightly from your experience. See "Choose a Certificate File" on page 842 for the latest information.

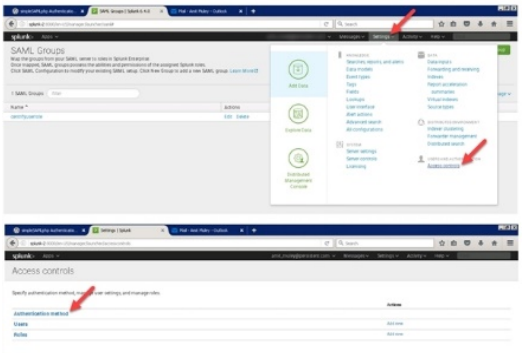
Configuring Splunk SSO

The following steps are specific to the Splunk application and are required in order to enable SSO for Splunk. For information on optional configuration settings available in the Delinea Admin Portal, see "Optional Configuration Settings" on page 844.

To configure Splunk for single sign-on:

1. In a new browser window, go to the Splunk server and sign in with your administrator login.

   > **Note:** It is helpful to open the Splunk web application and the Delinea Admin Portal Application Settings window simultaneously to copy and paste settings between the two browser windows.
2. In the Splunk server browser window, go to the **Settings** menu and select **Access Controls > Authentication method**.



3. Select **SAML** as your External Authentication Method.
4. Click **Configure Splunk to use SAML**.
5. On the SAML groups page, click **SAML Configuration**.
6. Configure the following **General Settings** in the Splunk application.

   The red arrows in the table below indicate the direction of the copy and paste operation between the two windows. For instance, the first arrow in the table below indicates that you copy the content from the indicated field on the Privileged Access Service Admin Portal and paste it into the corresponding field in the Splunk website

Admin Portal >Application Settings	Copy/Paste Direction	Splunk application	What you do
Download Identity Provider SAML Metadata	-->	Metadata XML File or Metadata Contents	Click Select File to Browse and select your Metadata file, or copy and paste the contents of the file directly into the Metadata Contents window. Note: If you do not know how to find your Metadata file, refer to your IdP's documentation. Note: Splunk supports SAML assertion based on the username value. The default template for Splunk On-Premise is configured to use the username format. The attribute used for this purpose is samAccountName. The Advanced Script however is designed to fetch user information from User repository in case the Privileged Access Service instance is not configured with the Active Directory.

Admin Portal >Application Settings	Copy/Paste Direction	Splunk application	What you do
N/A	N/A	Single Sign on URL	This field is populated automatically by your Privileged Access Service Metadata file. It is the protected endpoint on your IdP to which Splunk sends authentication requests. To access the login page after SAML is enabled, use the SSO Bypass URL: https://<YOUR-SPLUNK-FQDN:PORT>/account/login?loginType=Splunk
N/A	N/A	Single Log Out URL	This field is populated automatically by your Privileged Access Service Metadata file and is the IdP protocol endpoint. If you do not want users to be automatically logged out, remove the URL from this field.
Download Signing Certificate	N/A	IdP certificate path	You do not need to download this certificate. If you use the standard certificate, it is included as part of the Metadata file and no action is required here To use a different certificate with a private key (.pfx file), you can upload that certificate file to the Splunk application in the IdP's certificate path field. The value can be either a directory or a file, depending on your IdP requirements. If you provide a file, Splunk uses that file to validate the authenticity of SAML response. If you provide a directory, Splunk looks for all the certificates that are present as children of the directory and tries to validate SAML response with each one of them. If Splunk fails to validate authenticity with any of them, the SAML response is not considered authentic. If you replace the certificate, be sure to get a new Metadata file from Splunk that uses the new certificate.
Entity ID	N/A	Entity ID	This field is populated automatically by your Privileged Access Service Metadata file. The contents of this field on the Privileged Access Service Application Settings page must match the contents of this field in the Splunk application.
N/A	N/A	Sign AuthnRequest	Select this option.

Admin Portal >Application Settings	Copy/Paste Direction	Splunk application	What you do
N/A	N/A	Sign SAML Response	Select this option.

7. Skip the **Attribute Query Requests** section in the Splunk application.
8. In **Advanced Settings** in the Splunk application, configure the following settings:

Capability	Required?	What you do
Attribute Alias Role	Optional	Use this field to specify a role attribute sent from the IdP. Set the value as role. This value tells Splunk which attribute contains the role information in the SAML response returned.
Attribute Alias Mail	Optional	Use this field to specify a role attribute sent from the IdP. Set the value as emailaddress. This value maps the alias to the user email addresses in the SAML response returned.
Attribute Alias Real Name	Optional	Use this field to specify a role attribute sent from the IdP. Set the value as displayname. This value maps the alias to the user real names in the SAML response returned.
Fully qualified domain name or IP of the load balancer	Required	Set to the machine name with fully qualified domain name: https://acme.com. This setting works for a Splunk deployment with Single Search Head Setup or a Search Head Cluster Setup. You must provide an address if you use load balancing with a search head cluster.
Redirect port - load balancer port	Optional	Provide a redirect port for the load balancer described in the previous field.
Redirect to URL after logout	Optional	Provide a URL to redirect to after the user signs out.

9. Click **Save**.

   Note: For more information, see Configuring SSO with AzureAD or ADFS as your Identity Provider

10. (Optional) To turn on encryption (https), go to **Settings > Server Settings > General Settings** and select the **Yes** radio button for **Enable SSL (HTTPS) in Splunk Web**. For more information, see Splunk documentation.

!. Configure the following settings in the Admin Portal Application Settings window:

Admin Portal >Application Settings	Copy/Paste Direction	Splunk application	What you do
Assertion Consumer Service URL	N/A	N/A	This field will be automatically populated when you upload the Service Provider Metadata later during configuration. The URL is located in the AssertionConsumerService tag in the Metadata file. It should look similar to: http://< YOUR-SPLUNK-FQDN:PORT>/saml/acs. For example, If Splunk is installed on a machine with the IP address of 11.11.111.111 and a machine named splunk-1, then you can use either a URL with the IP address: http://11.11.111.111:8000/saml/acs/ or a URL with the machine name: http://splunk-1:8000/saml/acs Note: If you chose to enable SSL in the previous step, this URL must start with https instead of http.

Creating and uploading the Splunk Metadata in Admin Portal

Note: Uploading the Splunk Metadata file modifies the SAML assertion script. It is recommended that you copy and save your script before uploading the Splunk Metadata file.

Note: For more information about customizing scripts, see "Optional Configuration Settings" on page 844.

To upload Splunk Metadata in Admin Portal

1. In a new browser window, go to your Splunk Metadata file:

   https://*<YOUR-SPLUNK-FQDN:PORT>*/saml/spmetadata
2. Copy the contents of the Metadata file and paste it into a new file in a text editor.
3. Save the Metadata file with a file extension of .txt or .xml.
4. In the Admin Portal browser window, go to the **Advanced** page.

   Note: If you do not still have the browser window open that you were using in "Configuring Splunk SSO" on page 920, you may need to navigate to the Splunk app in Admin Portal and then Click on **Advanced** to navigate to the script page.
5. Copy the contents of the script window and save it into a file on your computer.
6. Click **Upload SP Metadata** and choose the Splunk Metadata file you created and saved above.
7. Copy and paste to replace the content of the script window with the script you saved before uploading the Metadata.

   Note: If you want to return your script to its original “factory installed” state, you can find the original script in "Splunk script" on page 927.
8. Click **User Access** in the Admin Portal and see "Deploying Applications" on page 839 for configuration details.

After you assign roles to the application, the application state changes to *deployed* and the assigned users can access the application.

9. Click **Account Mapping** in the Admin Portal and see "Map User Accounts" on page 840 for configuration details.
10. Click **Save** in Admin Portal.
11. Continue with "Mapping SAML groups to Splunk roles" below.

Mapping SAML groups to Splunk roles

To map SAML groups to Splunk roles:

1. In the Splunk web application browser window, go to the **SAML Groups** page.

   Note: If you do not still have the browser window open that you were using in "Configuring Splunk SSO" on page 920, you may need to navigate to the SAML Groups page by first opening the **Settings** menu and selecting **Access Controls > Authentication method**, then selecting **SAML as your authentication type** and clicking **Configure Splunk to use SAML**.

2. Click **New Group** to create a new group or click **Edit** to modify an existing group.
3. Provide a **Name** for the group.
4. Indicate the **Roles** that you want to assign to this group by moving the desired roles from the left column to the right column.
5. Click **Save**.

   Note: For more information, see Map SAML groups to roles.

   Now that you have finished configuring the application settings in the Admin Portal and the Splunk application, users are ready to launch the application from the Admin Portal.

For more information

- For more information about certificate chaining with Splunk, see Splunk documentation.
- For more information about configuring SSO with AzureAD or ADFS as your Identity Provider, see Splunk documentation.
- for more information about mapping SAML groups to roles, see Splunk documentation.
- Contact Splunk for more information about configuring Splunk On-Premise for SSO.

Splunk Specifications

Each SAML application is different. The following table lists features and functionality specific to Splunk.

Capability	Supported?	Support details
Web browser client	Yes	

Capability	Supported?	Support details
Mobile client	No	
SAML 2.0	Yes	
SP-initiated SSO	Yes	
IdP-initiated SSO	Yes	
Force user login via SSO only	Yes	After SSO is enabled, standard login forces users to login with SSO. To bypass SSO, login with this URL: https://<YOUR-SPLUNK-FQDN:PORT>/account/login?loginType=Splunk
Separate administrator login after SSO is enabled	Yes	Administrators can login separately using the SSO bypass URL: https://<YOUR-SPLUNK-FQDN:PORT>/account/login?loginType=Splunk
User or Administrator account lockout risk	No	After SAML is enabled, users can still login using the SSO bypass URL: https://<YOUR-SPLUNK-FQDN:PORT>/account/login?loginType=Splunk **Note:** After SAML is enabled, users without SAML-enabled accounts (user-password only) can only login with the bypass URL.
Automatic user provisioning	Yes	User is created in Splunk after successful consumption of SAML assertion.
Multiple User types	Yes	Admin User
Self-service password	Yes	Users can reset their own passwords only if they are non-provisioned users and have the change_own_password capability.
App Gateway	Yes	The App Gateway can be used to securely access this application outside of your corporate network. See "Configuring App Gateway" on page 980 for more information. **Note**: The App Gateway is a premium feature and is available only in the Privileged Access Service App+ Edition. Please contact your Privileged Access Service representative to have the feature enabled for your account.
Access restriction using a corporate IP range	Yes	You can specify an IP Range in the Admin Portal Policy page to restrict access to the application.

Splunk script

The following script is the original Splunk script provided in Admin Portal. Copying and pasting this script to the Advanced page in Admin Portal will return the script to its original “factory installed” state:

```
setIssuer(Issuer);

setSubjectName(UserIdentifier);

setAudience('splunkEntityId');

setRecipient(ServiceUrl);

setHttpDestination(ServiceUrl);

setSignatureType('Response');

setNameFormat('persistent');

if (ServiceUrl.match(/YOUR-SPLUNK-FQDN-AND-PORT/)) {

throw '_I18N_Exception_AcsUrlNotCompletelyConfigured';

}

var displayName = LoginUser.DisplayName;

if (!displayName) {

throw '_I18N_Exception_BadSamlAttributeValue';

}

var allRoles = new Array();

var groupNames = LoginUser.GroupNames;

for (var i = 0; i \< groupNames.Length; i++) {

allRoles.push(groupNames[i]);

}

var cloudRoles = LoginUser.RoleNames;

for (var i = 0; i \< cloudRoles.Length; i++) {

allRoles.push(cloudRoles[i]);

}

setAttributeArray('role', allRoles);
```

```
setAttribute('displayname', displayName);

setAttribute('emailaddress', UserIdentifier);
```

Sumo Logic

Sumo Logic offers both IdP-initiated SAML SSO (for SSO access through the Admin Portal) and SP-initiated SAML SSO (for SSO access directly through the Sumo Logic web application). You can configure Sumo Logic for either or both types of SSO.

Sumo Logic Requirements for SSO

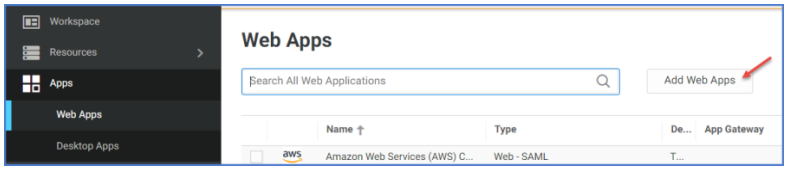
Before you configure the Sumo Logic web application for SSO, you need the following:

- An active Sumo Logic account for your organization.
- An Assertion Consumer Number ID assigned by Sumo Logic.
- A signed certificate.
- You can either download one from Admin Portal or use your organization's trusted certificate.
- Contact information for Sumo Logic support (to enable and test the SSO feature on your account).

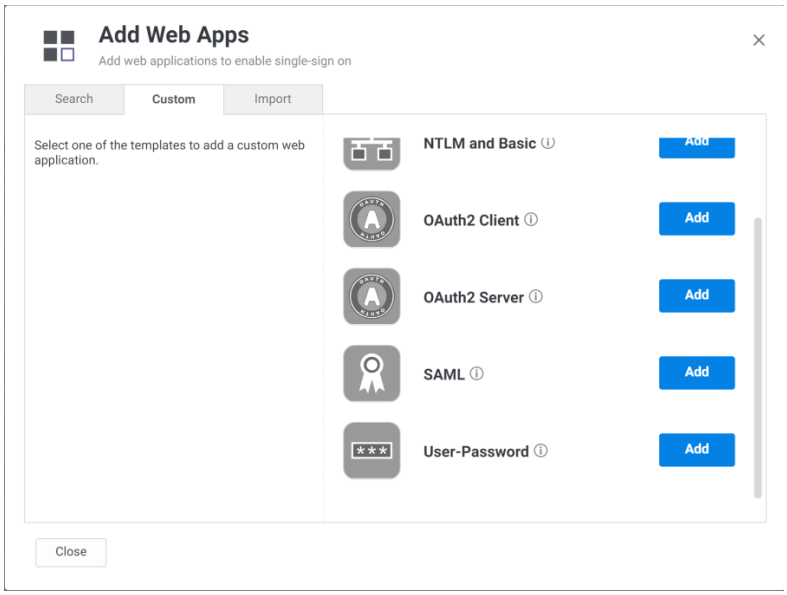
Adding Sumo Logic in Admin Portal

To add the Sumo Logic application in Admin Portal:

1. In Admin Portal, click **Apps**, then click **Add Web Apps**.



   The Add Web Apps screen appears.
2. On the Search tab, enter the partial or full application name in the Search field and click the search icon.

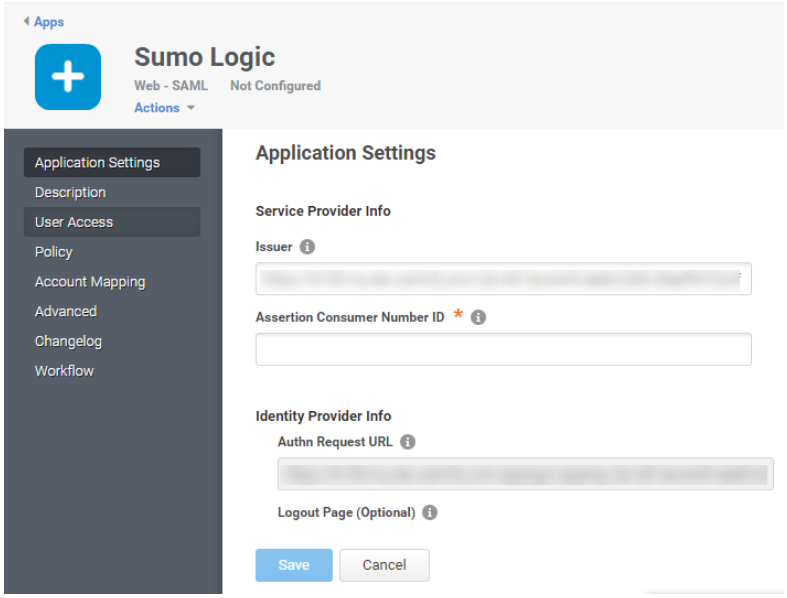


3. Next to the application, click **Add**.
4. In the Add Web App screen, click **Yes** to confirm.

   Admin Portal adds the application.
5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Application Settings page.

   Note: The description of how to choose and download a signing certificate in this document might differ slightly from your experience. See "Choose a Certificate File" on page 842 for the latest information.



6. Keep this browser tab open to the Application Settings page for the Sumo Logic app.

Configuring Sumo Logic for Single Sign-On

The following steps are specific to the Sumo Logic application and are required in order to enable SSO for Sumo Logic. For information on optional configuration settings available in the Centrify Admin Portal, see "Optional Configuration Settings" on page 844.

To configure Sumo Logic for SSO:

1. In a new browser window, go to the following URL and sign in as Admin:

   https://service.sumologic.com

   > **Note:** It is helpful to open the Sumo Logic web application and the Centrify Admin Portal Application Settings window simultaneously to copy and paste settings between the two browser windows.

2. Go to **Manage > Security**.
3. Click the **SAML** button.
4. Copy and paste the following information from the Sumo Logic web page to the Application Settings page in Admin Portal

   The red arrows in the tables below indicate the direction of the copy and paste operation between the two windows. For instance, the first arrow in the table below indicates that you copy the content from the indicated field on the Sumo Logic website and paste it into the corresponding field in the Privileged Access Service Admin Portal.

Admin Portal >Application Settings	Copy/Paste Direction	Sumo Logic web application	What you do
Assertion Consumer Number ID		N/A	Enter the Assertion Consumer Number ID you received from Sumo Logic. If your Assertion Consumer URL is https://service.sumologic.com/sumo/saml/consume/123456, enter 123456 here.

5. Select a configuration or create a new one and click **Configure**.
6. Enter the name of your organization as the **Configuration Name**.
7. Configure the following settings (in the Sumo Logic web application and the Centrify Admin Portal Application Settings window):

Admin Portal >Application Settings	Copy/Paste Direction	Sumo Logic web application	What you do
Issuer		Issuer	Copy the Issuer from Admin Portal and paste it here.

Admin Portal >Application Settings	Copy/Paste Direction	Sumo Logic web application	What you do
Authn Request URL			Copy the Authn Request URL from Admin Portal and paste it here.
Download Signing Certificate		X.509 Certificate	1. Click Download Signing Certificate on the Application Settings page in Admin Portal. 2. Open the file in a text editor. 3. Copy the entire contents of the file. 4. Paste it here.
Logout Page	 (Optional)	Logout Page	1. Check the box for Logout Page. 2. Copy the Logout Page from Admin Portal and paste it here.
Roles Attribute	 (Optional)	Roles	1. Check the box for Roles Attribute. 2. Enter roles. 2. Make sure it has the same name as the setAttribute with the role names to be set in the script on the Advanced page in Admin Portal.

8. Click **Account Mapping** in the Admin Portal and see "Map User Accounts" for configuration details.
9. Click **Save**.

Sumo Logic Specifications

Each SAML application is different. The following table lists features and functionality specific to Sumo Logic.

Capability	Supported?	Support details
Web browser client	Yes	
Mobile client	No	
SAML 2.0	Yes	
SP-initiated SSO	Yes	
IdP-initiated SSO	Yes	
Force user login via SSO only	No	Username-password login remains available after SSO is enabled.
Separate administrator login after SSO is enabled	No	

Capability	Supported?	Support details
User or Administrator lockout risk	No	
Automatic user provisioning	Yes	Log in to https://service.sumologic.com as Administrator and go to **Manage > Security** to configure On Demand provisioning.
Multiple User Types	Yes	Admin user End users
Self-service password	Yes	Users can reset their own passwords. Resetting another user's password requires administrator rights.
Access restriction using a corporate IP range	Yes	You can specify an IP Range in the Admin Portal Policy page to restrict access to the application.

Adding Desktop App Sets

After you have added desktop apps, you can organize them into logical groups—desktop app sets—to simplify management activity and reporting for attributes in common.

To add a desktop app set:

1. In the Admin Portal, click **Apps**, then click **Desktop Apps** to display the list of desktop applications.
2. In the Sets section, click **Add** to create a new set.
3. Type a name for the new set, an optional description, and select whether group membership is manual or dynamic.

   For manual sets, you can specify permissions for both the set itself and the members of the set. For dynamic sets, you can only specify permissions on the set.
4. Identify the members of the set in one of two ways.
   - If set membership is **Dynamic**, type the SQL statement to execute to identify set members in the **Query** field. For example, if you want to add a set for the applications with a name that starts with ora, you could type a SQL statement like this:

     select id from Application where Name like 'ora%'
   - If you select **Manual**, click **Members**, then click **Add** to search for and select the desktop applications to add as members.
5. Click **Save**.

   Also see, "Managing Application Sets" on page 830.

Adding Desktop Apps Using the Admin Portal

The Desktop App feature in Delinea Privileged Access Service launches a Windows application (for instance, applications such as SQL Server Management Studio, TOAD for Oracle, and VMware vSphere Client) on an instance of a Windows Server.

The Desktop App feature is built on RemoteApp from Microsoft Remote Desktop Services (formerly known as Terminal Services), to stream the application running on the Windows Server to the user's endpoint. User credentials are passed to the application so users do not need to checkout passwords. Desktop applications are configured from the Delinea Admin Portal and are also launched from the Admin Portal. Delinea Privileged Access Service controls:

- Who can use the feature.
- Which instance of Windows Server is targeted to run Remote Desktop Services.
- The account context for the target desktop and application.
- The command line used to launch the application (this may include account credentials for the application and a connection target such as an SQL Server database).

> **Note:** To prevent users from launching additional applications within a desktop app session, Microsoft best practice is to use AppLocker to control which applications are allowed within a session. For more information on AppLocker, see https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd759117(v=ws.11).

Microsoft Windows Server runs the remote desktop and the application for the user using Remote Desktop Services. Microsoft requires you to have the appropriate licensing in place for Remote Desktop Services. Delinea does not provide the Remote Desktop Services licenses; you must get the licenses directly from Microsoft. In order to use the Windows RemoteApp feature, the following Microsoft licenses must be available for every Windows/domain user configured to log in to the host Windows Server:

- A Client Access License (CAL) for Microsoft Windows Server.

  This licenses the configured user to log in to an instance of the Windows Server and launch both the desktop and the application.
- A Client Access License (CAL) for Microsoft Remote Desktop Services.

  This licenses the configured user to stream the remote desktop session to their computer.

You will need one of each of these licenses for each configured user (not concurrent user). Depending on your environment and Microsoft licensing, you may be able to choose between user CAL (for configured users) or device CAL (for Delinea connectors). Check with your Microsoft licensing specialist.

For additional information, see the following licensing guidance from Microsoft:

- https://www.microsoft.com/en-us/licensing/product-licensing/client-access-license.aspx
- https://blogs.technet.microsoft.com/tip_of_the_day/2017/02/22/rds-tip-of-the-day-license-your-rds-deployment-with-client-access-licenses-cals/

For more information about adding and managing specific desktop apps, see the following topics:

- "SQL Server Management Studio" on the next page
- "TOAD for Oracle" on page 937
- "VMware vSphere Client" on page 940
- "Generic Desktop App" on page 943
- "Selecting Actions for Desktop Apps" on the next page

- "Adding Desktop App Sets" on page 932 and "Managing Application Sets" on page 830

  Note: For the Privileged Access Service implementation of keyboard shortcuts for desktop apps, see Using the default web-based client.

Selecting Actions for Desktop Apps

Click anywhere in the row that contains the desktop app name to display application configuration details. Click the check box next to the application to view the available list of Actions for the application. The same actions are also available from the Actions menu when you click the desktop app. You can select the following actions:

Launch to log in to the desktop app with the configured credentials. For information on the available keyboard shortcuts, see Using the default web-based client.

Add To Set to add the selected desktop app to a new or existing set. Also see "Adding Desktop App Sets" on page 932 and "Managing Application Sets" on page 830.

Delete to remove a desktop app from the list. You cannot delete desktop apps that have an active session.

After you have added desktop apps, you can organize them into logical groups—desktop app sets—to simplify management activity and reporting for attributes in common.

SQL Server Management Studio

Add SQL Server Management Studio to your desktop app catalog to allow Privileged Access Service administrators to configure which users are allowed to connect to SQL database instances that reside on a remote application host system. Users can log in to remote desktop applications with specified credentials and without having to checkout a password. Delinea Privileged Access Service uses standard command-line architecture to pass account parameters and credentials to desktop applications running under remote desktop services. Additionally, detailed information about user activity on the host application system can be captured on the systems you choose to audit.

SQL Server Management Studio Prerequisites

Before you configure Desktop Applications in the Admin Portal for remote access, you need to make sure your environment meets the following requirements:

- A standalone Windows Server with Remote Desktop Services deployed. In Remote Desktop Services, you need to:
  - Publish the desktop application to your remote desktop collection.
  - Configure desktop application parameters to *Allow any command*line parameters*. This enables the Privileged Access Service command line functionality.

    Note: Delinea recommends that you do not run remote desktop services on the same Windows Server that includes the Delinea Connector.
- One or more of the following Privileged Access Service administrator rights to access the Apps tab in Admin Portal (also see Admin Portal administrative rights):
  - Privileged Access Service User
  - Privileged Access Service Power User

  - Privileged Access Service Administrator
- The application host must have **View** permission.
- *Application Management* administrator right to access **Apps** > **Add Desktop Apps**.
- Desktop App administrator has **Grant** permissions for account objects that are specified as arguments in a command line.
- If you configure the remote desktop app host login to use Shared account credentials, the Desktop App administrator must have **Grant** permission for the user associated with the Shared Host Login account.
- An active SQL Server Management Studio account with the following minimum permissions: *Login* permissions to the target SQL Server Management Studio Server instance and *Connect* permissions to the target SQL Server Management Studio Database.

Configuring SQL Server Management Studio

The following steps are specific to this application and are required in order to manage application access to SQL Server Management Studio.

1. In the Admin Portal. click **Apps**, and then **Desktop Apps** to add the SQL Server Management Studio application.
2. Click Add Desktop App to open the Add Desktop Apps wizard.
3. Next to the application you want to add, click **Add**.

   You can also use the Search tab to find an application. Enter the partial or full application name in the Search field and click the search icon.
4. In the Add Desktop App screen, click **Yes** to confirm.
5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Application Settings page.
6. On the **Application Settings** page, specify the following settings:

Option	Description
Application Host	To add an application host system with a database instance: Click **Select** next to the Application Host text box to select the relevant remote host system. Start typing the system name into the search box and select the system you want to add. Systems that you have View rights to are displayed. Click **Done**. The relevant remote host system is displayed in the text box.

Option	Description
Host Login Credentials	Select one of the following log in methods to be used when launching the RDP connection to the application host system: User's Active Directory credential Select this option to allow users to log in to the application host system using their AD credentials. To configure this option you also need to make sure that **Securely capture users passwords at login** is enabled in **Settings > Authentication > Security Settings**. Select Alternative Account Select this option to allow users to log in to the application host system using their alternative account. If only one alternative account is available, then selecting **Launch** from the Admin Portal proceeds directly to a login screen. If more than one alternative account is available, you need to first select which account to use to log in to the application host system, and then click **Continue**. For information on alternative accounts, see Discovering alternative accounts. Prompt for username and password Select this option to allow users to log in to the application host system using their own Windows credentials. Selecting **Launch** from the Admin Portal, prompts the user for their Windows User Name and Password. Shared Account Select this option to allow users to log in to the application host system using shared accounts. Administrators must have the Grant permission for the shared account in order to configure the account for access. Selecting this option means that all users use the same shared account in order to access the application host system. Delinea recommends that you use a different Windows account for each Desktop App configuration using a shared account to avoid session conflicts. Click **Select** next to the Shared Account text box to select the relevant account. Start typing the system name into the search box. Available shared accounts are displayed. Select the shared account you want to have access to the host system. Click **Done**. The shared account is displayed in the text box.

7. Locate the Alias name in the remote desktop server (Server Manager > Remote Desktop Services > Alias column) for the published application and enter the information into Application Alias field in the Admin Portal.

   Note: The default setting for SQL Server Management Studio is **Ssms**. If your configuration does not use the default alias, you will need to modify the default setting to reflect your configuration.

8. (Optional) Select the database and user account arguments to be used in the command line when launching the application host system.

   These arguments instruct the application host system how to access the application and replace the placeholders in the command line string below.

Argument	Description
database	To configure the database argument: Click **Select** in the database row to select the relevant database. Start typing the database name into the search box. Available databases are displayed. Click the database that you want to access. Click **Select**.
user	To configure the user argument: Click **Select** in the user row to select a relevant user account. Start typing the account name into the search box. Available user accounts are displayed. Click the user name that you want to have access to the application host system. Click **Select**.

9. (Optional) Enter command line arguments for {database.FQDN}\{database.InstanceName} {user.User} {user.Password} in the command string.

   Linked object placeholders are available and are displayed as {argumentName.linkedObjectAttribute}.

   This field, when configured with the command line arguments, passes the credential and target database information to the desktop application on how to launch and log in to the application host system. Use the command line arguments in the field above to replace the placeholders in the string provided. When you launch the application the placeholders are replaced with the specified database and user arguments.

10. (Optional) On the **Description** page, you can:
    - Add a unique name and description for each supported language instance.
    - Change the name, description, and logo for the application.

11. Configure the following Desktop App pages as needed. Click **Save** at the bottom of each page to save your changes.
    - Permissions–Assigning permissions
    - Policy–"Specifying Additional Authentication Control"
    - Workflow–"Managing Application Access Requests" on page 823
    - Changelog–"Viewing a Log of Recent Changes"

      For information on actions available for Desktop Apps, see "Selecting Actions for Desktop Apps" on page 934.

TOAD for Oracle

Add TOAD for Oracle to your desktop app catalog to allow Privileged Access Service administrators to configure which users are allowed to connect to database instances that reside on a remote application host system. Users can log in to remote desktop applications with specified credentials and without having to checkout a password. Delinea Privileged Access Service uses standard command-line architecture to pass account parameters and credentials to desktop applications running under remote desktop services. Additionally, detailed information about user activity on the host application system can be captured on the systems you choose to audit.

TOAD for Oracle Prerequisites

Before you configure Desktop Applications in the Admin Portal for remote access, you need to make sure your environment meets the following requirements:

- A standalone Windows Server with Remote Desktop Services deployed. In Remote Desktop Services, you need to:
  - Publish the desktop application to your remote desktop collection.
  - Configure desktop application parameters to *Allow any command-line parameters*. This enables the Privileged Access Service command line functionality.

    Note: Delinea recommends that you do not run remote desktop services on the same Windows Server that includes the Delinea Connector.

- One or more of the following Privileged Access Service administrator rights to access the Apps tab in Admin Portal (also see Admin Portal administrative rights):
  - Privileged Access Service User
  - Privileged Access Service Power User
  - Privileged Access Service Administrator
- The application host must have **View** permission.
- *Application Management* administrator right to access **Apps** > **Add Desktop Apps**.
- Desktop App administrator has **Grant** permissions for account objects that are specified as arguments in a command line.
- If you configure the remote desktop app host login to use Shared account credentials, the Desktop App administrator must have **Grant** permission for the user associated with the Shared Host Login account.
- An Oracle database account that can connect to the target Oracle database.

Configuring TOAD for Oracle

The following steps are specific to this application and are required in order to manage application access to TOAD for Oracle.

1. In the Admin Portal. click **Apps**, and then **Desktop Apps** to add the SQL Server Management Studio application.
2. Click Add Desktop App to open the Add Desktop Apps wizard.
3. Next to the application you want to add, click **Add**.

   You can also use the Search tab to find an application. Enter the partial or full application name in the Search field and click the search icon.
4. In the Add Desktop App screen, click **Yes** to confirm.
5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Application Settings page.
6. On the **Application Settings** page, specify the following settings:

Option	Description
Application Host	To add an application host system with a database instance: Click **Select** next to the Application Host text box to select the relevant remote host system. Start typing the system name into the search box and select the system you want to add. Systems that you have View rights to are displayed. Click **Done**. The relevant remote host system is displayed in the text box.

Option	Description
Host Login Credentials	Select one of the following log in methods to be used when launching the RDP connection to the application host system: User's Active Directory credential Select this option to allow users to log in to the application host system using their AD credentials. To configure this option you also need to make sure that **Securely capture users passwords at login** is enabled in **Settings > Authentication > Security Settings**. Select Alternative Account Select this option to allow users to log in to the application host system using their alternative account. If only one alternative account is available, then selecting **Launch** from the Admin Portal proceeds directly to a login screen. If more than one alternative account is available, you need to first select which account to use to log in to the application host system, and then click **Continue**. For information on alternative accounts, see Discovering alternative accounts. Prompt for username and password Select this option to allow users to log in to the application host system using their own Windows credentials. Selecting **Launch** from the Admin Portal, prompts the user for their Windows User Name and Password. Shared Account Select this option to allow users to log in to the application host system using shared accounts. Administrators must have the Grant permission for the shared account in order to configure the account for access. Selecting this option means that all users use the same shared account in order to access the application host system. Delinea recommends that you use a different Windows account for each Desktop App configuration using a shared account to avoid session conflicts. Click **Select** next to the Shared Account text box to select the relevant account. Start typing the system name into the search box. Available shared accounts are displayed. Select the shared account you want to have access to the host system. Click **Done**. The shared account is displayed in the text box.

7. Locate the Alias name in the remote desktop server (Server Manager > Remote Desktop Services > Alias column) for the published application and enter the information into Application Alias field in the Admin Portal.

   Note: The default setting for TOAD for Oracle is **Toad**. If your configuration does not use the default alias, you will need to modify the default setting to reflect your configuration.

8. (Optional) Select the database and user account arguments to be used in the command line when launching the application host system.

   These arguments instruct the application host system how to access the application and replace the placeholders in the command line string below.

Argument	Description
database	To configure the database argument: Click **Select** in the database row to select the relevant database. Start typing the database name into the search box. Available databases are displayed. Click the database that you want to access. Click **Select**.
user	To configure the user argument: Click **Select** in the user row to select a relevant user account. Start typing the account name into the search box. Available user accounts are displayed. Click the user name that you want to have access to the application host system. Click **Select**.

9. (Optional) Enter command line arguments for {user.User}/{user.Password}@{database.FQDN}:{database.Port}/{database.ServiceName} in the command string.

   Linked object placeholders are available and are displayed as {argumentName.linkedObjectAttribute}.

   This field, when configured with the command line arguments, passes the credential and target database information to the desktop application on how to launch and log in to the application host system. Use the command line arguments in the field above to replace the placeholders in the string provided. When you launch the application the placeholders are replaced with the specified database and user arguments.

10. (Optional) On the **Description** page, you can:
    - Add a unique name and description for each supported language instance.
    - Change the name, description, and logo for the application.

11. Configure the following Desktop App pages as needed. Click **Save** at the bottom of each page to save your changes.
    - Permissions–Assigning permissions
    - Policy–"Specifying Additional Authentication Control"
    - Workflow–"Managing Application Access Requests" on page 823
    - Changelog–"Viewing a Log of Recent Changes"

For information on actions available for Desktop Apps, see "Selecting Actions for Desktop Apps" on page 934.

VMware vSphere Client

Add VMware vSphere Client to your desktop app catalog to allow Privileged Access Service administrators to configure which users are allowed to connect to the remote desktop application host system. Users can log in to remote desktop applications with specified credentials and without having to checkout a password. Delinea Privileged Access Service uses standard command-line architecture to pass account parameters and credentials to desktop applications running under remote desktop services. Additionally, detailed information about user activity on the host application system can be captured on the systems you choose to audit.

VMware vSphere Client Prerequisites

Before you configure Desktop Applications in the Admin Portal for remote access, you need to make sure your environment meets the following requirements:

- A standalone Windows Server with Remote Desktop Services deployed. In Remote Desktop Services, you need to:
  - Publish the desktop application to your remote desktop collection.
  - Configure desktop application parameters to *Allow any command-line parameters*. This enables the Privileged Access Service command line functionality.

    Note: Delinea recommends that you do not run remote desktop services on the same Windows Server that includes the Delinea Connector.

- One or more of the following Privileged Access Service administrator rights to access the Apps tab in Admin Portal (also see Admin Portal administrative rights):
  - Privileged Access Service User
  - Privileged Access Service Power User
  - Privileged Access Service Administrator
- The application host must have **View** permission.
- *Application Management* administrator right to access **Apps** > **Add Desktop Apps**.
- Desktop App administrator has **Grant** permissions for account objects that are specified as arguments in a command line.
- If you configure the remote desktop app host login to use Shared account credentials, the Desktop App administrator must have **Grant** permission for the user associated with the Shared Host Login account.

The VMware vSphere Client supports VMware VMkernel systems with a VMkernel system version below 6.5. During application host configuration, you can select defined VMware VMkernel systems and local accounts in the Privileged Access Service. Note that the local account credential type must be a password; not an SSH key.

Configuring VMware vSphere Client

The following steps are specific to this application and are required in order to manage application access to VMware vSphere Client.

1. In the Admin Portal. click **Apps**, and then **Desktop Apps** to add the SQL Server Management Studio application.
2. Click Add Desktop App to open the Add Desktop Apps wizard.
3. Next to the application you want to add, click **Add**.

   You can also use the Search tab to find an application. Enter the partial or full application name in the Search field and click the search icon.
4. In the Add Desktop App screen, click **Yes** to confirm.
5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Application Settings page.
6. On the **Application Settings** page, specify the following settings:

Option	Description
Application Host	To add an application host system with a database instance: Click **Select** next to the Application Host text box to select the relevant remote host system. Start typing the system name into the search box and select the system you want to add. Systems that you have View rights to are displayed. Click **Done**. The relevant remote host system is displayed in the text box.

Option	Description
Host Login Credentials	Select one of the following log in methods to be used when launching the RDP connection to the application host system: User's Active Directory credential Select this option to allow users to log in to the application host system using their AD credentials. To configure this option you also need to make sure that **Securely capture users passwords at login** is enabled in **Settings > Authentication > Security Settings**. Select Alternative Account Select this option to allow users to log in to the application host system using their alternative account. If only one alternative account is available, then selecting **Launch** from the Admin Portal proceeds directly to a login screen. If more than one alternative account is available, you need to first select which account to use to log in to the application host system, and then click **Continue**. For information on alternative accounts, see Discovering alternative accounts. Prompt for username and password Select this option to allow users to log in to the application host system using their own Windows credentials. Selecting **Launch** from the Admin Portal, prompts the user for their Windows User Name and Password. Shared Account Select this option to allow users to log in to the application host system using shared accounts. Administrators must have the Grant permission for the shared account in order to configure the account for access. Selecting this option means that all users use the same shared account in order to access the application host system. Delinea recommends that you use a different Windows account for each Desktop App configuration using a shared account to avoid session conflicts. Click **Select** next to the Shared Account text box to select the relevant account. Start typing the system name into the search box. Available shared accounts are displayed. Select the shared account you want to have access to the host system. Click **Done**. The shared account is displayed in the text box.

7. Locate the Alias name in the remote desktop server (Server Manager > Remote Desktop Services > Alias column) for the published application and enter the information into Application Alias field in the Admin Portal.

   Note: The default setting for VMware vSphere Client is **VpxClient**. If your configuration does not use the default alias, you will need to modify the default setting to reflect your configuration.

8. (Optional) Select the server, user account, and secret arguments to be used in the command line when launching the application host system.

   These arguments instruct the application host system how to access the application and replace the placeholders in the command line string below.

Argument	Description
server	To configure the server argument, click **Select** in the server row to select the a VMware VMkernel system previously added to the Privileged Access Service.
user	To configure the user argument, click **Select** in the user row to select a local Privileged Access Service account.

9. (Optional) Enter command line arguments for {server}, {user.User} and {user.Password} in the command string.

Two types of placeholders are available; value type and linked object. A value type argument is displayed as {argumentName} , and a linked object is displayed as {argumentName.linkedObjectAttribute}.

This field, when configured with the command line arguments, passes the credential information to the desktop application on how to launch and log in to the application host system. Use the command line arguments in the field above to replace the placeholders in the string provided. When you launch the application the placeholders are replaced with the specified server, user, and secret arguments.

10. (Optional) On the **Description** page, you can:
    - Add a unique name and description for each supported language instance.
    - Change the name, description, and logo for the application.
11. Configure the following Desktop App pages as needed. Click **Save** at the bottom of each page to save your changes.
    - Permissions—Assigning permissions
    - Policy—"Specifying Additional Authentication Control"
    - Workflow—"Managing Application Access Requests" on page 823
    - Changelog—"Viewing a Log of Recent Changes"

      For information on actions available for Desktop Apps, see "Selecting Actions for Desktop Apps" on page 934.

Generic Desktop App

If you'd like to add a desktop applications that aren't in our Delinea Desktop App Catalog, you can create custom application profiles using the generic application template. Custom application profiles provide user access to desktop applications that may not be open to the general public or that haven't yet been added to the app catalog.

Adding a Generic desktop app to your desktop app catalog allows Privileged Access Service administrators to configure which users are allowed to connect to desktop applications that reside on a remote application host system. Users can log in to remote desktop applications with specified credentials and without having to checkout a password. Delinea Privileged Access Service uses standard command-line architecture to pass account parameters and credentials to desktop applications running under remote desktop services. Additionally, detailed information about user activity on the host application system can be captured on the systems you choose to audit.

Generic Desktop App Prerequisites

Before you configure Desktop Applications in the Admin Portal for remote access, you need to make sure your environment meets the following requirements:

- A standalone Windows Server with Remote Desktop Services deployed. In Remote Desktop Services, you need to:
  - Publish the desktop application to your remote desktop collection.
  - Configure desktop application parameters to *Allow any command-line parameters*. This enables the Privileged Access Service command line functionality.

> **Note:** Delinea recommends that you do not run remote desktop services on the same Windows Server that includes the Delinea Connector.

- One or more of the following Privileged Access Service administrator rights to access the Apps tab in Admin Portal (also see Admin Portal administrative rights):
  - Privileged Access Service User
  - Privileged Access Service Power User
  - Privileged Access Service Administrator
- The application host must have **View** permission.
- *Application Management* administrator right to access **Apps** > **Add Desktop Apps**.
- Desktop App administrator has **Grant** permissions for account objects that are specified as arguments in a command line.
- If you configure the remote desktop app host login to use Shared account credentials, the Desktop App administrator must have **Grant** permission for the user associated with the Shared Host Login account.

Configuring Generic Desktop Apps

The following steps are specific to the generic desktop application template and are required in order to manage application access.

1. In the Admin Portal. click **Apps**, and then **Desktop Apps** to add the SQL Server Management Studio application.
2. Click Add Desktop App to open the Add Desktop Apps wizard.
3. Next to the application you want to add, click **Add**.

   You can also use the Search tab to find an application. Enter the partial or full application name in the Search field and click the search icon.
4. In the Add Desktop App screen, click **Yes** to confirm.
5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Application Settings page.
6. On the **Application Settings** page, specify the following settings:

Option	Description
Application Host	To add an application host system with a database instance: Click **Select** next to the Application Host text box to select the relevant remote host system. Start typing the system name into the search box and select the system you want to add. Systems that you have View rights to are displayed. Click **Done**. The relevant remote host system is displayed in the text box.

Option	Description
Host Login Credentials	Select one of the following log in methods to be used when launching the RDP connection to the application host system: User's Active Directory credential Select this option to allow users to log in to the application host system using their AD credentials. To configure this option you also need to make sure that **Securely capture users passwords at login** is enabled in **Settings > Authentication > Security Settings**. Select Alternative Account Select this option to allow users to log in to the application host system using their alternative account. If only one alternative account is available, then selecting **Launch** from the Admin Portal proceeds directly to a login screen. If more than one alternative account is available, you need to first select which account to use to log in to the application host system, and then click **Continue**. For information on alternative accounts, see Discovering alternative accounts. Prompt for username and password Select this option to allow users to log in to the application host system using their own Windows credentials. Selecting **Launch** from the Admin Portal, prompts the user for their Windows User Name and Password. Shared Account Select this option to allow users to log in to the application host system using shared accounts. Administrators must have the Grant permission for the shared account in order to configure the account for access. Selecting this option means that all users use the same shared account in order to access the application host system. Delinea recommends that you use a different Windows account for each Desktop App configuration using a shared account to avoid session conflicts. Click **Select** next to the Shared Account text box to select the relevant account. Start typing the system name into the search box. Available shared accounts are displayed. Select the shared account you want to have access to the host system. Click **Done**. The shared account is displayed in the text box.

7. Locate the Alias name in the remote desktop server (Server Manager > Remote Desktop Services > Alias column) for the published application and enter the information into Application Alias field in the Admin Portal.
8. (Optional) Click **Add** to select the command-line arguments to be used when launching the application host system.

   These arguments instruct the application host system how to access the application and replace the placeholders in the command line string (described below). Once added, you can either click Select to choose from available options or click the edit icon to add relevant information. You can define multiple arguments for the same type. For details on the available arguments and their descriptions, see the information icon next to the field in the Admin Portal.
9. (Optional) Enter a custom command line string that uses the arguments defined in the Command Line Arguments field.

   The command line string you configure is flexible and is dependent upon the requirements of the target application. Two types of placeholders are available; value type and linked objects. A value type argument is displayed as {argumentName} , and a linked object is displayed as {argumentName.linkedObjectAttribute}.

   This field, when configured with the command line arguments, passes information to the desktop application on how to launch and log in to the application host system. Use the command line arguments in the field above to replace the placeholders in the string provided. When you launch the application the placeholders are replaced with the arguments you specify.

10. (Optional) On the **Description** page, you can:
    - Add a unique name and description for each supported language instance.
    - Change the name, description, and logo for the application.
11. Configure the following Desktop App pages as needed. Click **Save** at the bottom of each page to save your changes.
    - Permissions–Assigning permissions
    - Policy–"Specifying Additional Authentication Control"
    - Workflow–"Managing Application Access Requests" on page 823
    - Changelog–"Viewing a Log of Recent Changes"

For information on actions available for Desktop Apps, see "Selecting Actions for Desktop Apps" on page 934

Adding Custom Applications

This section describes how to add, configure, and deploy custom applications using the Admin Portal.

Working with custom applications "Adding Custom Applications" above "Custom User-password Applications" on page 955"Custom SAML Applications" on page 961"Custom OAuth2 Client" on page 969"Custom OAuth2 Server" on page 972"Adding User-password Applications" on page 975"OpenID Connect" below

OpenID Connect

Introduction

Delinea provides support for many different federation standards. OpenID Connect is a popular federation standard that is supported by Delinea. This document provides an overview of how OpenID Connect works, describes how to configure an application in the Administrator Portal, and describes how to authenticate users programmatically in applications.

Terminology

To understand how authentication works, you need to know the following terms and acronyms:

- **Client:** An application, such as a website or a mobile application used to access Delinea.

  Note: The client is not the user. (The user is the person using the client application.)

- **Client ID:** A unique identifier that an authorization service issues to identify a client application. The authorization service generates the client ID when the service registers the application. The authorization service uses the client ID and client Secret in subsequent API requests to ensure that the client can access an online resource.
- **Client Secret:** A unique code that an authorization service issues when the service registers the application. You can think of it as the password for the client application. The client Secret and the client ID enable the client to access an online resource.
- **Identity Provider (IDP):** A service provider that authenticates a user on behalf of another service provider.

- **OpenID Connect Provider (OP):** A service provider (Delinea) that implements OpenID Connect as an authentication mechanism.
- **Relying party (RP):** Another name for a client. This term is sometimes used in descriptions of authorization processes.
- **Single Sign-On (SSO):** The ability of a user to sign on (authenticate) once, then access multiple online applications without having to sign on to each of them individually.

OpenID Connect Overview

The Problem

An application that accesses protected resources on behalf of users must be able to verify that users are who they claim to be.

You could enable an application to verify users by creating a database of usernames and passwords, but using a database is unsatisfactory. It is time-consuming, it requires your users to register and remember the usernames and passwords, and it requires your client application and server to access the usernames and passwords.

The Solution

A better solution is to leverage an existing, trustworthy identity provider (IDP) that can authenticate large volumes of users, and that your users are already registered with (for example, Google). Using an IDP allows your users to log in with existing credentials that they already know and use, while keeping those user credentials secret from your application.

Delinea supports OpenID Connect, a single sign on (SSO) standard that allows you to authenticate users by using an existing IDP to provide access to applications managed through the Delinea PAS. Delinea is, therefore, an OpenID Connect Provider (OP).

OpenID Connect is built upon another standard, OAuth 2.0, which was designed for granting authorization permissions to users for resources exposed over the web (for example, REST endpoints). OpenID Connect provides two layers of security: user authentication (verifying the user) and user authorization (allowing access to specific resources). OpenID Connect is also built on HTTP/JSON, is RESTful, and is compatible with both web and mobile applications.

When you develop an application with the Delinea PAS, OpenID Connect allows you to leverage an IDP to authenticate users of your application. Once authenticated, your users can then access the resources (for example, applications) for which you granted authorization. Most importantly, the authorization aspect of OpenID Connect allows this authorization to be sent downstream, thus facilitating SSO for all of the applications that users are authorized to access.

Note: Although authentication and authorization are two separate security aspects, from a technical standpoint, OpenID Connect implements authentication as an OAuth 2.0 authorization request behind the scenes, whereby the authorization requests the user's identity. This means that OpenID Connect implements authentication by making a call to the OAuth 2.0 authorization endpoint, which supplies the user's ID token. OpenID Connect uses that ID token, in conjunction with the authorization token (access token) obtained earlier from the token endpoint, to authorize access to resources such as applications.

The End Goal

When you authenticate a user in your client application (the relying party), the result provided by an OP (for example, Delinea) includes two important tokens (encoded numbers), collectively called the Token, used to make subsequent API calls on behalf of the user:

- **ID token:** An ID identifying the user. This is retained by a client (for example, stored in a cookie) so that it can be used to authenticate in subsequent API calls. Storing it allows for stateless sessions.
- **Access token:** An ID specifying the user's authorization permissions for resources.

You obtain the ID token and access token by using authorization flows. The authorization flow you use depends on the type of client application you are writing. OAuth 2.0, and therefore, OpenID Connect, support three authorization flows:

- **Authorization Code flow:** Use the Authorization (Auth) Code Flow flow for applications that can maintain the secrecy of a client secret (for example, server-side JavaScript). The OpenID Provider (OP) issues a temporary authorization code in a backchannel (for example, it is not exposed to the user), once the user is authenticated. The client (the application) sends this authorization code to a token endpoint on the OP. The OP, in turn, returns the final ID and access tokens to the client (again through a back channel).

  Note: The application's client secret is also sent to help ensure that only authorized client applications can request an access token.

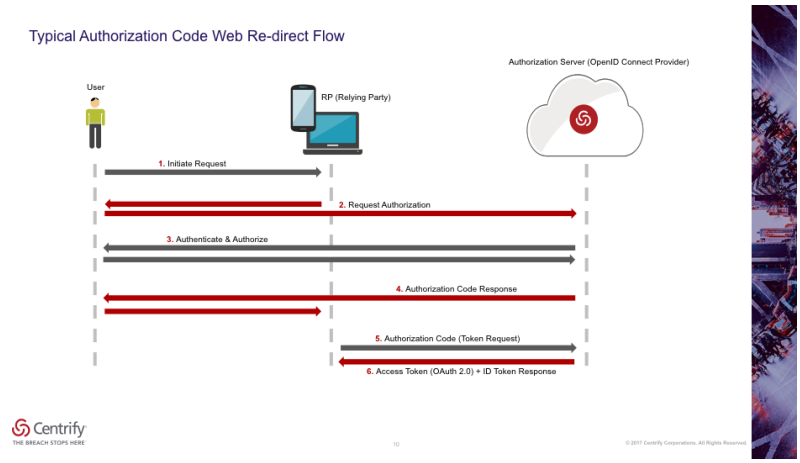
- **Implicit flow:** Use the Implicit Flow flow for applications that cannot maintain the secrecy of a client secret (for example, browser-based applications). The application obtains an access token directly in an authorization request (via a redirect), over a secure communication channel, with no intermediate authorization code requested or returned.
- **Hybrid flow:** Use a combination of the previous two authorization flows for applications that can maintain the secrecy of a client secret, but don't require the use of a client ID/secret.

How it Works

The following diagram illustrates the basic authentication flow. The main actors are the user, the RP (your client application that the user is accessing), and Delinea (the OP that performs as an authorization server).

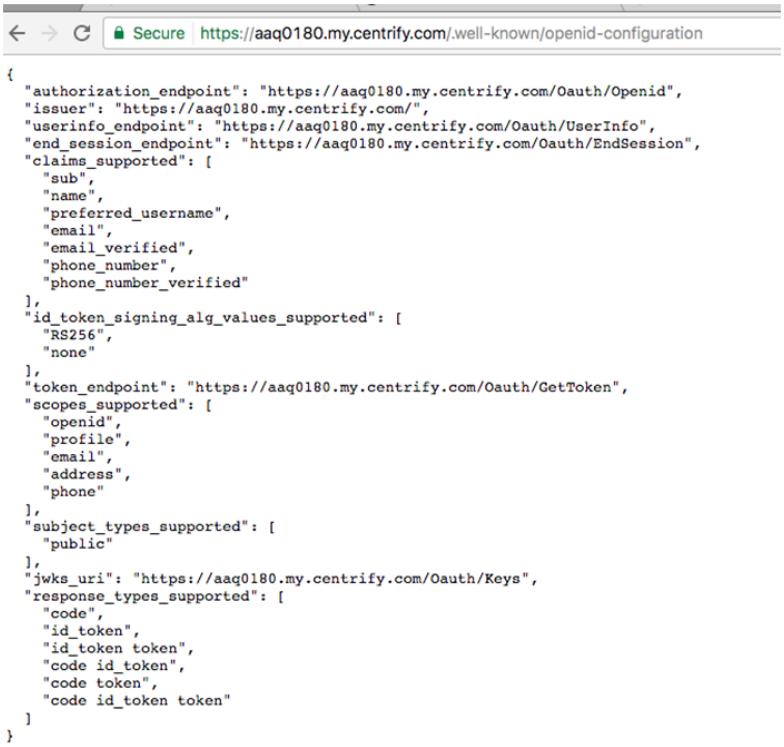
In this example, a user initiates a request through your client application to start SSO. Your application redirects the user to an IDP user interface that allows the user to enter credentials. The redirection information includes your application's client ID, client secret, and the location to go to once the user has successfully authenticated (for example, another screen on your website).

Upon successful authentication, the OP returns a temporary authorization code to your client application. This authorization code is opaque to your client application. That is, your client application cannot interpret the authorization code in any way. Because your application obtains this authorization code instead of direct client credentials, your user's credentials are hidden from your application. Your client application then sends this temporary authorization code back to the OP. The OP then returns the Authorization Token and ID Token that your client application can use to make subsequent API calls.



An OP (for example, Delinea) consists of, or provides, the following endpoints. An OP is, therefore, often referred to as an Authorization Server:

- **Authorization endpoint:** The OAuth 2.0 authorization endpoint of an IDP that provides the UI for the user to log in to. A client redirects a user to this end point to authenticate and authorize the user.
- **Token endpoint:** The end point that authenticates a client application and allows it to exchange an access code for the token.
- **Userinfo endpoint:** An endpoint that a client can use to get information about a user once authenticated. This information includes whatever information the user shares in their user configuration.
- **Provider metadata:** A JSON document containing the OP's endpoint information for a tenant and the supported OpenID Connect/OAuth 2.0 features. A client application can use this to dynamically configure requests to the OP. As shown in the following example, metadata can be obtained by entering your tenant's base URL and appending it with /.well-known/openid-configuration:



Example Request Responses

The following HTTP query parameters redirect the user to an IDP:

- scope is set to open_id (authorization code flow) to indicate that this authorization request is requesting the user identity (for authentication purposes)
- client_id
- response_type is set to code to indicate that the authorization code flow is to be used.

Example authentication redirection to the OP:

HTTP/1.1 302 Found

Location: https://openid.c2id.com/login?response_type=code&scope=openid&client_id=s6BhdRkqt3&state=af0ifjaldkj&redirect_url=https%3A%2F%2Fclient.example.orf%Fcb

The following request parameters are encoded in the URI query:

- response_type: Set to code to indicate an authorization code flow.
- scope: The scope of the requested authorization in OAuth. The scope value openid signals a request for OpenID authentication and ID token.

- client_id: The client identifier of the RP at the OP. This identifier is typically obtained when the RP is registered with the OP, via the client registration API, developer console, or some other method.
- state: The opaque value set by the RP to maintain state between request and callback.
- redirect_uri: The RP callback URI for the authentication response.

Delinea also supports the optional prompt query parameter defined by OpenID Connect Core 1.0 that controls whether the authorization server prompts the end user for reauthentication and consent. This can be set to the following values:

- none: the authorization server must not display any type of authentication prompt.
- login: the authorization server should display an authentication prompt for reauthentication. If it cannot authenticate the user then a login_required error is returned.

https://openid.c2id.com/login?response_type=code&scope=openid&client_
id=s6BhdRkqt3&state=af0ifjaldkj&prompt=login&redirect_url=https%3A%2F%2Fclient.example.orf%Fcb

The following figure shows the HTTP query parameters that the OP uses to redirect the user to the site that was specified in the previous call after the IDP authenticates the user. This response includes the temporary authorization code and any state information that was provided by the client in the previous API request.

The OP will then call the client redirect_uri with an authorization code (on success) or an error code (if access was denied, or some other error occurred, such as a malformed request).

HTTP/1.1 302 Found

Location: https://client.example.org/cb?code=Sp1x10BezQQybYS6WxSbIA&state=af0ifjsldkj

The RP must validate the state parameter and use the code to proceed to the next step, exchanging the code for the ID token.

The following example shows the HTTP request header and body that is sent from the client to the OP's Token endpoint to request the token. The body includes the temporary authorization code returned from the previous API call.

POST /token HTTP/1.1

Host: openid.c2id.com

Content-Type: application/x-www-form-urlencoded

Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2jW

grant_type=authorization_code&code=Sp1x1OBeZQQYbYS6WxSbIA&redirect_
uri=https%3A%2F%2Fclient.example.org%2Fcb

The client ID and secret are passed via the authorization header. Apart from HTTP basic authentication, OpenID Connect also permits authentication with signed JWT assertions, which do not expose the client secret with the token request, and hence offer better security.

The token request parameters are form encoded:

- grant_type: set to authorization_code.
- code: the code obtained from the first step.
- redirect_uri: repeats the callback URI from the first step.

The following example shows an HTTP response body containing the token. The token_type of bearer indicates that the client can use and have full access to that token.

On success the OP will return a JSON object with an ID token, access token, and optional refresh token:

HTTP/1.1 200 OK

Content-Type: application/json

Cache-Control: no-store

Pragma: no-cache

{

"id_token" : "erJHbGciOasfkhawkjehkjasdladsliajwefkjaASDFAEFAWEijias..."

"access_token" : "S1AV32hkKg"

"token_type" : "Bearer",

"expires_in": 3600

}

The following example shows the HTTP response body from a request the client made to the Userinfo endpoint, to request information about the user who was authenticated. The information includes previously consented user profile information, so a valid access token is required.

Note: The Userinfo is JSON encoded and may optionally be packaged as a JWT that is signed or encrypted.

GET /userinfo HTTP/1.1

Host: openid.c2id.com

Authorization: Bearer S1AV32hkKG

The UserInfo is JSON encoded and may optionally be packaged as a JWT that is signed or encrypted.

HTTP/1.1 200 OK

Content-Type: application/json

{

"sub" : "alice",

"email" : "alice@wonderland.net",

"email_verified" : true,

"name" : "Alice Adams",

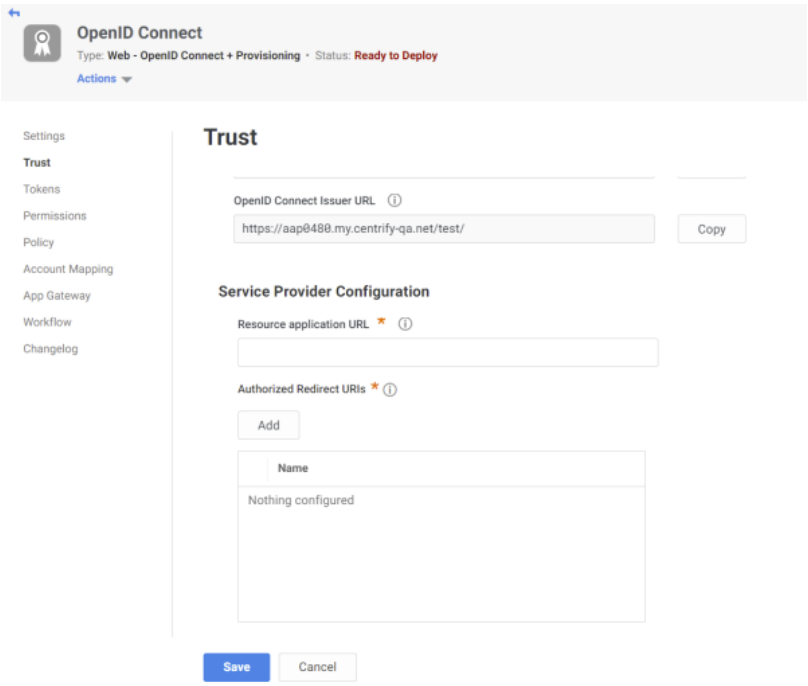
"picture" : "https://c2id.com/users/alice.jpg"

}

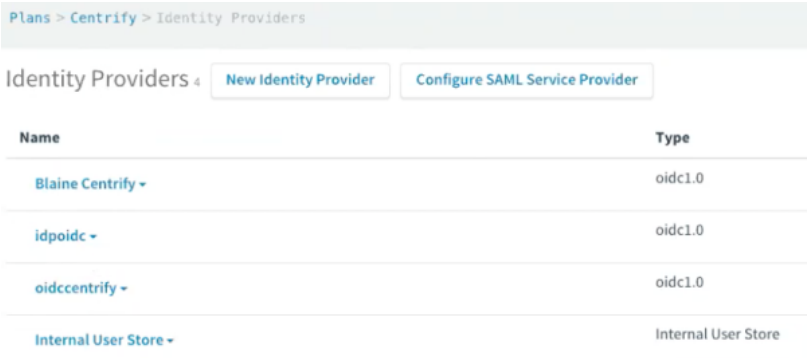
Server Side Configuration

To make this all work, you must configure your client application on the OP. Some elements (for example, client ID and secret) must match in the server-side and client-side configurations.

The following image shows the Delinea Dashboard, where you configure a client application. The Resource application URL field specifies the URL where the user logs in. The Authorized Redirect URLs field specifies the location to redirect the user to, once the user is authenticated. The Identity Provider Info fields specify the application's auto-generated client ID, metadata URL, and Issuer URL. The client secret must be manually entered into these fields.



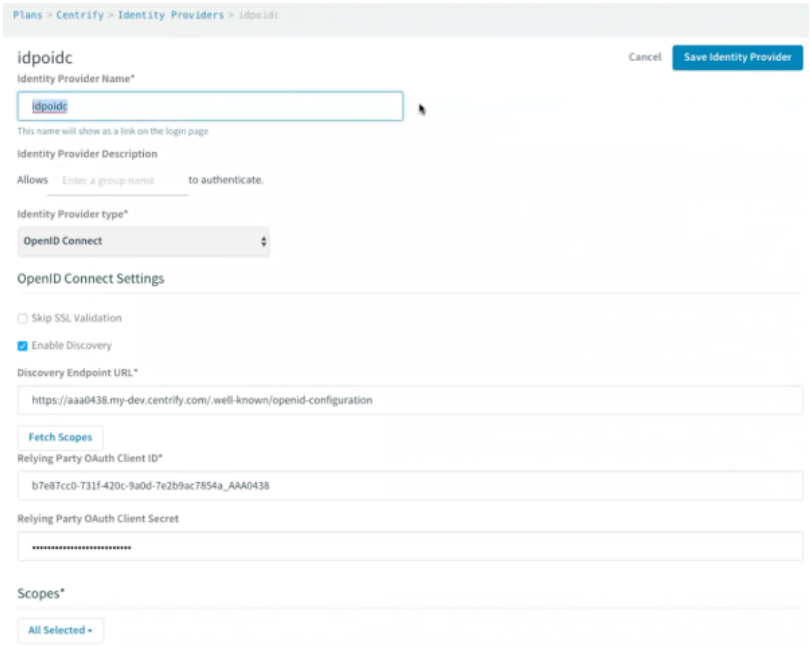
The following figure shows a list of IDPs configured on Delinea. You can configure a new IDP from this screen, and you can edit existing IDP configurations.



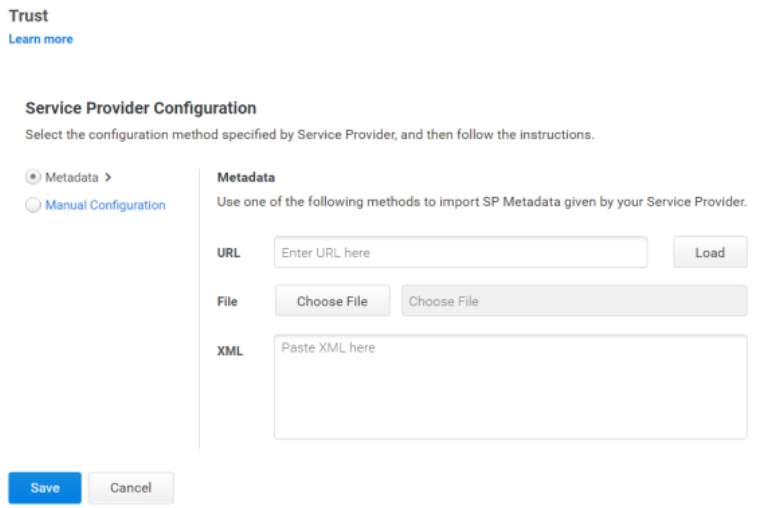
The following figure shows the editing of an IDP configuration for an RP.

1. Set the **Identity Provider Type** to **OpenID Connect** to use OpenID Connect authentication.
2. Select **Enable Discovery** to make the IDP pull all OP information from the provider metadata endpoint.

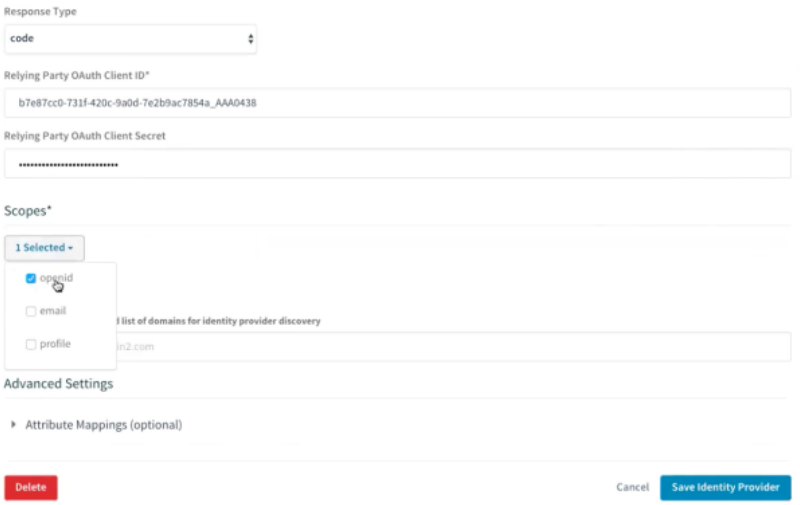
3. Use the **Relying Party OAuth Client ID** and **Relying Party OAuth Client Secret** fields to authenticate the client application itself with the IDP.



If you disable **Enable Discovery**, you must manually enter all of the OP information in the fields shown in the following figure:



Select the **Scope**, which must include **openid**. This corresponds to the scope that the RP sends to the OP when it starts the authentication process, as mentioned above. You can optionally select additional scope as well to provide other types of information.



Additional Resources

- OAuth Mobile and Native Apps
- OpenID Connect Explained

Custom User-password Applications

If you'd like to add applications that aren't in our Delinea App Catalog, you can create custom application profiles using the generic application templates. Custom application profiles provide user access through the Admin Portal to applications that may not be open to the general public or that haven't yet been added to the app catalog.

These instructions describe the basic steps for using the generic user-password application template. They show how to create a custom application profile to a web application that uses a user name and a password for authentication. For full instructions on creating a custom user-password application connection, read the "User-Password Application Scripting" on page 1024.

Adding and Configuring a Custom User-password Application

To add a custom user-password application

1. In Admin Portal, click **Apps**, then click **Add Web Apps**.

   The Add Web Apps screen appears.
2. Click **Custom**.
3. On the Custom tab, next to the **User-Password** application, click **Add**.
4. In the Add Web App screen, click **Yes** to add the application.

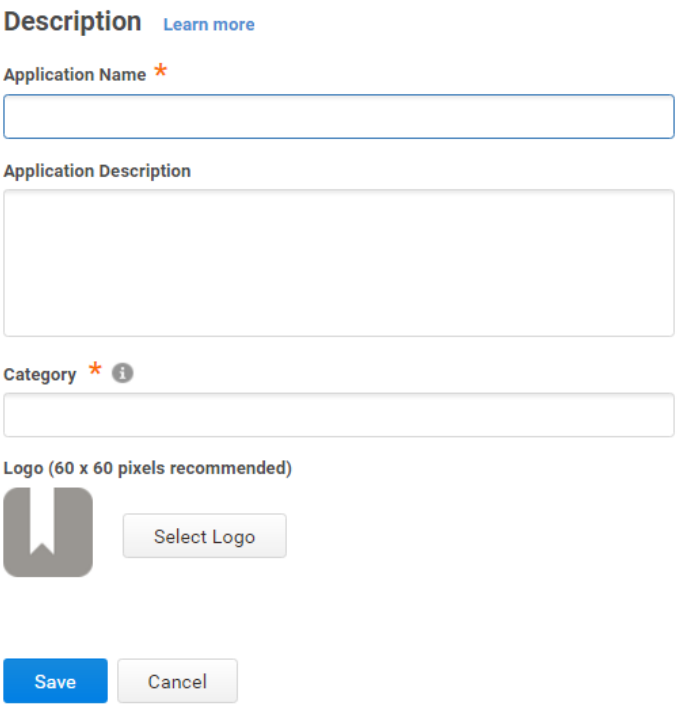
   Admin Portal adds the application.
5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Application Settings page.
6. Enter the web application's login URL in the URL field.

7. (Optional) If the web application has a login URL that is designed for viewing on mobile devices, enter that address in the Mobile URL field.

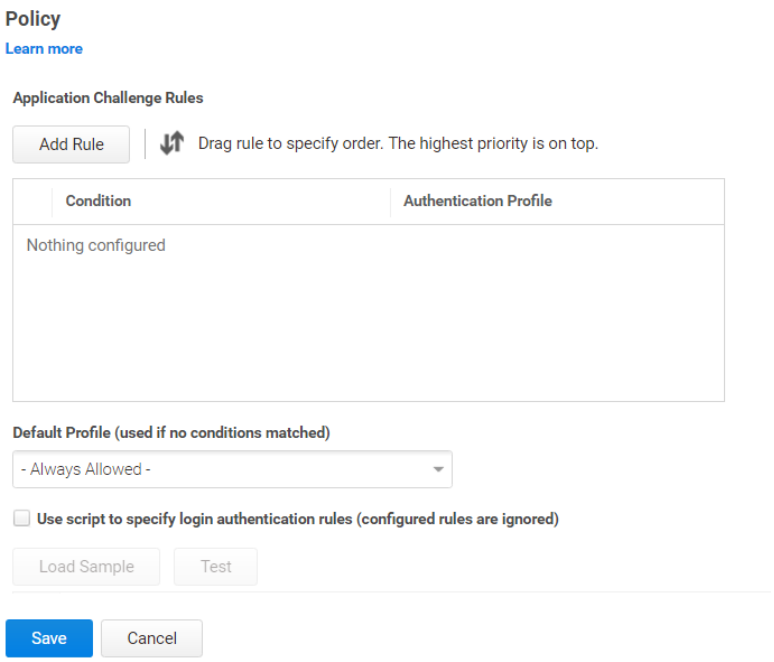
   When a user on a mobile device requests this web application, the connection request goes to the mobile URL. If there is no mobile URL, a mobile device connection request goes to the standard URL in the field above. All requests from standard browsers go to the standard URL.

8. On the **Description** page, change the name and description for the application.

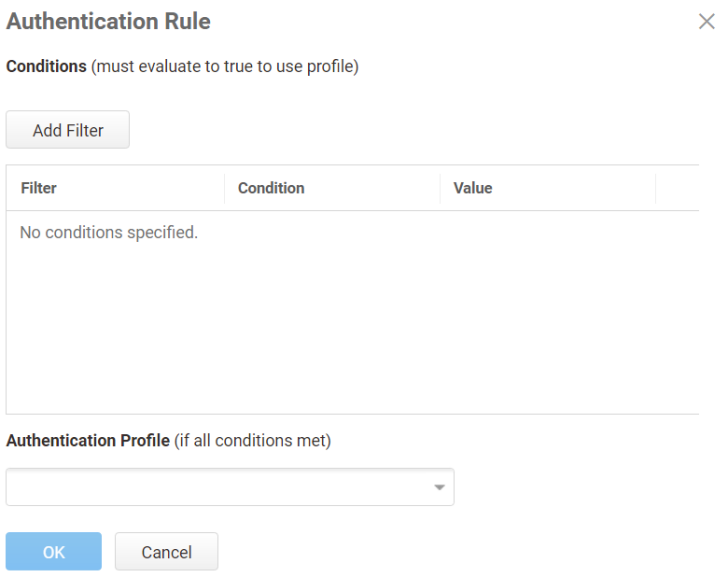


   Because this is a generic or custom application, it's recommended to give this application a unique name. You can also provide a custom application logo.

9. (Optional) On the Policy page, specify additional authentication controls for this application.



a. Click **Add Rule**.
The Authentication Rule window displays.



b. Click **Add Filter** on the Authentication Rule window.

c. Define the filter and condition using the drop-down boxes.
For example, you can create a rule that requires a specific authentication method when users access the

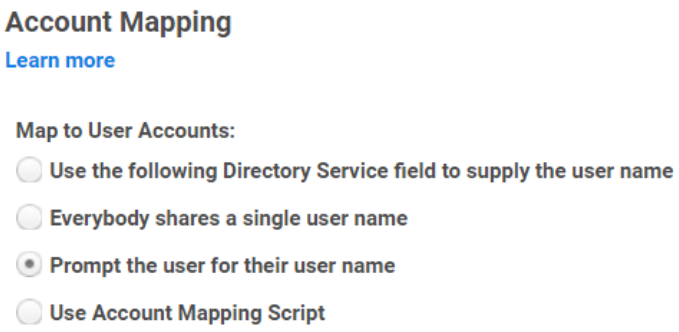
Privileged Access Service from an IP address that is outside of your corporate IP range. Supported filters are:

Filter	Description
IP Address	The authentication factor is the computer's IP address when the user logs in. This option requires that you have configured the IP address range in Settings, Network, Corporate IP Range.
Identity Cookie	The authentication factor is the cookie that is embedded in the current browser by the Privileged Access Service after the user has successfully logged in.
Day of Week	The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.
Date	The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.
Date Range	The authentication factor is a specific date range.
Time Range	The authentication factor is a specific time range in hours and minutes.
Device OS	The authentication factor is the device operating system.
Browser	The authentication factor is the browser used for opening the Privileged Access Service Admin Portal.
Country	The authentication factor is the country based on the IP address of the user computer.
For the Day/Date/Time related conditions, you can choose between the user's local time and Universal Time Coordinated (UTC) time.	

10. Click the **Add** button associated with the filter and condition.
11. Select the profile you want applied if all filters/conditions are met in the **Authentication Profile** drop-down. The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the **Add New Profile** option. See Creating authentication profiles
12. Click **OK.**

13. (Optional) In the **Default Profile (used if no conditions matched)** drop-down, you can select a default profile to be applied if a user does not match any of the configured conditions.
    If you have no authentication rules configured and you select **Not Allowed** in the **Default Profile** dropdown, users will not be able to log in to the service.
14. Click **Save**.
    If you have more than one authentication rule, you can prioritize them on the **Policy** page. You can also include JavaScript code to identify specific circumstances when you want to block an application or you want to require additional authentication methods. For details, see "Application Access Policies with JavaScript" on page 987.

    Note: If you left the Apps section of Admin Portal to specify additional authentication control, you will need to return to the Apps section before continuing by clicking **Apps** at the top of the page in Admin Portal.
15. On the **Account Mapping** page, configure how the login information is mapped to the application's user accounts.



- **Use the following Directory Service field to supply the user name**: Use this option if the user accounts are based on user attributes. For example, specify an Active Directory field such as *mail* or *userPrincipalName* or a similar field from Delinea Directory.

  For Web - User Password applications, selecting this option allows an additional option to let Active Directory users log in using Active Directory credentials. Select the **Use the login password supplied by the user (Active Directory users only)** option for every Web - User Password application that you want users to log in to using Active Directory credentials.
- **Everybody shares a single user name**: Use this option if you want to share access to an account but not share the user name and password. For example, some people share an application developer account.
- **Prompt the user for their user name**: Use this option if you want users to supply their own user name and password. The first time a user launches the application, they enter their login credentials for that application. The Privileged Access Service stores the user name and password and the next time the user

launches the application, the Privileged Access Service logs the user in automatically.

LoginUser.Username = LoginUser.Get('mail')+'.ad';

The above script instructs the Privileged Access Service to set the login user name to the user's mail attribute value in Active Directory and add '.ad' to the end. So, if the user's mail attribute value is Adele.Darwin@acme.com then the Privileged Access Service uses Adele.Darwin@acme.com.ad. For more information about writing a script to map user accounts, see "User-Password Application Scripting" on page 1024.

Note: When the user first logs in to the application, the Admin Portal will ask for the application's login password and then (if the script hasn't already created a password) store the application password in the Privileged Access Service so it's not required for later logins by the user.

The options are as follows:

16. On the **Advanced** tab, click **Edit** to enter or modify the JavaScript that specifies the HTML login response that the Privileged Access Service sends to the web application login URL when a user requests the application. This advanced script must be present and configured to match the service provider's required form fields.

    The default example script shows how to specify form fields. The example script does *not* work as is, and you must modify the script to match each application's form field requirements. For the vast majority of web applications, you need to replace only the username-field in line 2 with the form field name you discovered earlier for user name, replace the password-field in line 4 with the form field name you discovered for the password, and then delete lines 6 and 7.

    An example (without comment lines) using the form field names User and Password:

    response.AddFormField("User", encode(LoginUser.Username));

    response.AddFormField("Password", encode(LoginPassword));

    For detailed information about writing an advanced script and for descriptions of the objects and methods provided by the Privileged Access Service for defining an HTTP login response, read "User-Password Application Scripting" on page 1024.

17. (Optional) Click **App Gateway** to allow users to securely access this application outside of your corporate network. For detailed configuration instructions, see "Configuring App Gateway" on page 980.

    Note: The App Gateway feature is a premium feature and is available only in the Privileged Access Service App+ Edition. Please contact your Delinea representative to have the feature enabled for your account.

18. (Optional) On the **Changelog** page, you can see recent changes that have been made to the application settings, by date, user, and the type of change that was made.

19. (Optional) Click **Workflow** to set up a request and approval work flow for this application.

    See "Managing Application Access Requests" on page 823 for more information.

20. Click **Save**.

Custom Apps Overview

To use the generic user-password application template, you must be able to write or modify a simple JavaScript script.

How to use the generic user-password template (an overview):

1. Discover the login URL where the user-password web application accepts authentication requests and the names of the form data fields used to accept user name and password. Do this using POST analysis in a web browser (described later).
2. Add “Generic User-Password” to the application list in the Admin Portal and open its entry to configure the template.
3. Use the general user-password application template to configure the basics of a new user-password application profile: application name, an icon, the login URL for authentication, a way to determine the user name, and so on.
4. Write or modify an advanced script in JavaScript that specifies form data field names for the web application and assigns user name and password values to the appropriate fields.
5. Specify roles that have access to the custom user-password application.
6. Save the new custom user-password application profile so that it appears with its new name in Admin Portal’s application list.

Discovering the Login URL and Form Data Fields

This example of how to discover a user-password web application’s login URL and its form data fields requires a browser capable of analyzing http requests.

To discover an application’s login URL and form data fields:

1. In your browser, go to a user-password web application’s login page.
2. Open your browser’s network analyzer tool, typically found under Developer Tools, or something similar.
3. Enter your credentials in the login page and click the login button.
4. Look for the Logon POST method and select it.
5. View the login header.
6. Look within the header for “Request URL.” This is the request URL. You’ll use its value for the URL field in the generic user-password application template.
7. Look within the header for the “Form Data” section, then within that section for the user name field and the password field. The fields may have many different names depending on how the application defined them. You can identify the user name field because its value will be your user name. The password field’s value will be your password. You’ll use these two field names in the advanced script in the generic user-password application template.

   Note: If you keep the browser and its development tools open, you can cut and paste the request URL and form data field names from the browser into the generic user-password application template.

Custom SAML Applications

If you’d like to add applications that aren’t in our catalog or aren't publicly available, you can use the Custom SAML application.

With Privileged Access Service, you can choose single-sign-on (SSO) access to your Custom SAML web application with IdP-initiated SAML SSO (for SSO access through the Admin Portal) or SP-initiated SAML SSO (for

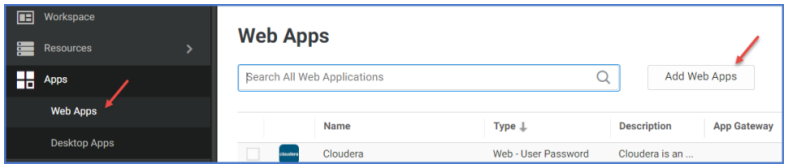
SSO access directly through the Custom SAML web application) or both. Providing both methods gives you and your users maximum flexibility.

These instructions describe the steps for using the Custom SAML application template to configure and deploy your application. They show how to create a custom application profile to a web application that uses SAML (Security Assertion Markup Language) for authentication. Refer to "SAML Application Scripting" on page 1001 for more information about writing the scripts in this template.

Note: To use the Custom SAML application template, it is highly recommended that you first understand the basics of SAML and JavaScript. You will have to provide required SAML information to the web application's service provider, as well as possibly modify a script in JavaScript to specify a SAML assertion for each user log-on with the web application. Also see "Introduction to Application Management" on page 823 for a description of the SAML workflow.

To Add and Configure a Custom SAML Application

1. In Admin Portal, click **Apps**, then click **Add Web Apps**.



   The Add Web Apps screen appears.

2. Click **Custom**.
3. On the Custom tab, next to the **SAML** application click **Add**.
4. In the Add Web App screen, click **Yes** to add the application.

   Admin Portal adds the application.

5. Click **Close** to exit the Application Catalog.

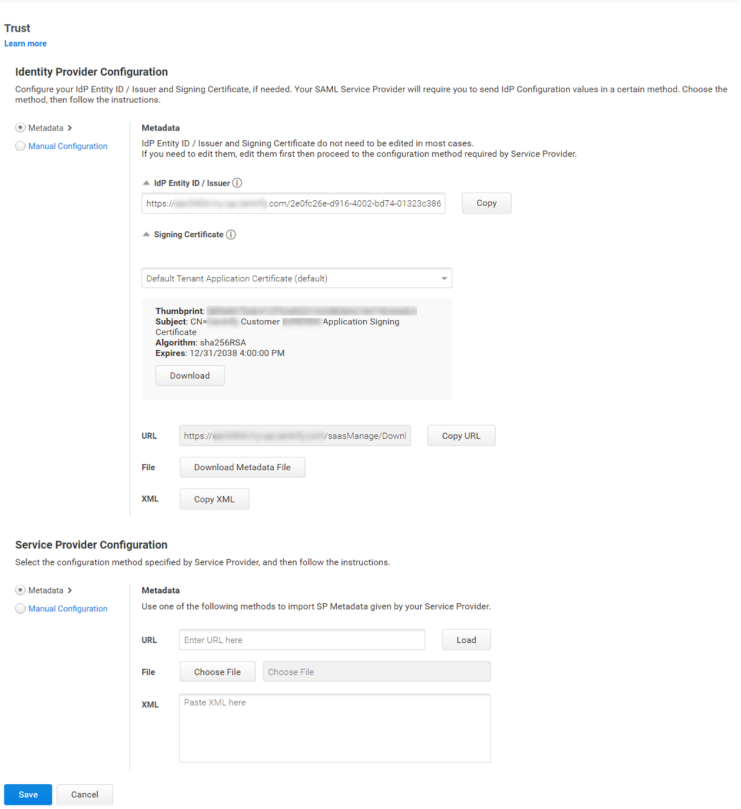
   The application that you just added opens to the Settings page.

6. Click **Trust** to go to the Trust page.

   The Trust page contains fields and controls for SAML information that might be required by the web application Service Provider. You must supply this information in the format requested by the Service Provider.

   The Trust page is divided into two parts:

   - Identity Provider Configuration
   - Service Provider Configuration



The next steps provide the information about the SAML information available on the Trust page, broken down by section for both Metadata and Manual Configuration.

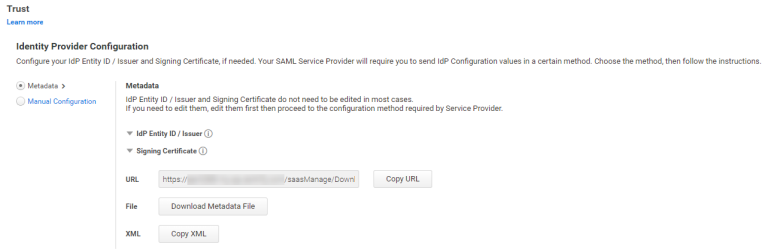
7. Update the information for the Identify Provider Configuration section, the click **Save**.

   The only change that might be required in the identity Provider Configuration section is changing the signing certificate.

   Description of Identity Provider Configuration Metadata fields

Option	Description
Identify Provider Configuration	
Metadata (selected)	

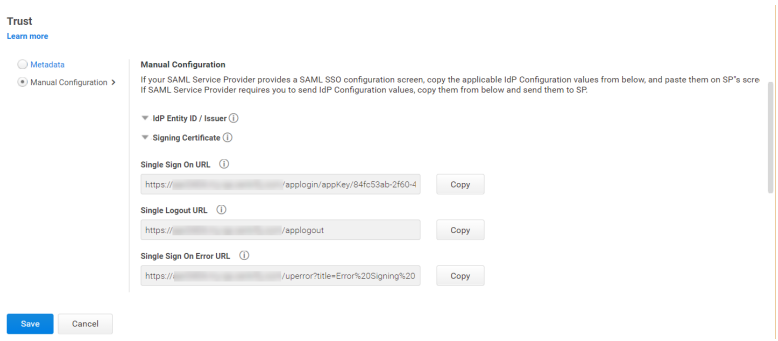
Option	Description
IdP Entity ID / Issuer	The IdP Entity ID can also be referred to as an Issuer. A URL unique to this application profile. This value is the entity ID used in the SAML assertion to identify the identity provider attempting to authenticate. The web application doesn't contact this URL so it need not be functional.
Signing Certificate	These settings specify the signing certificate used for secure SSO authentication between the Privileged Access Service and the web application. Just be sure to use a matching certificate both in the application settings in the Admin Portal and in the application itself. Select an option to change the signing certificate. Use the Default Tenant Application Certificate (default) Select this option to use the Privileged Access Service standard certificate. This is the default setting. Click Download to save the certificate so you can use it during the application configuration process. If you replace the certificate, be sure to update application with the new certificate information. -Upload New Signing Certificate- Select this option to upload your organization's own certificate. To use your own certificate, you must enter a name and a password (if the file requires a password) and then click Browse to upload an archive file (.p12 or .pfx extension) that contains the certificate along with its private key. Upload the certificate from your local storage prior to downloading any IdP metadata. If the IdP metadata is available from a URL, be sure to upload the certificate prior to providing the URL to your service provider.
URL	The information for the certificate that you have selected is shown in the URL field. Click Copy URL to easily copy the address of the certificate. Use this URL to configure your SAML application (this is similar to downloading the metadata and sending it to the service provider but instead you just provide the URL). This method can be used as an alternative to downloading the metadata. The method used depends on service provider requirements.
File	Click Download Metadata File to download SAML metadata in an XML file. The metadata contains the security certificate and other SAML information that you can provide to the service provider. For Business Partner Federation, this is the information that you need to provide to the service provider/host.
XML	Click Copy XML to copy the XML content. This is similar to downloading the metadata and sending it to the service provider but instead you just provide the XML content. This method can be used as an alternative to downloading the metadata. The method used depends on service provider requirements.



Description of Identity Provider Configuration Manual Configuration fields

Option	Description
Identify Provider Configuration	
Manual Configuration (selected)	
IdP Entity ID / Issuer	The IdP Entity ID can also be referred to as an Issuer. A URL unique to this application profile. This value is the entity ID used in the SAML assertion to identify the identity provider attempting to authenticate. The web application doesn't contact this URL so it need not be functional.
Signing Certificate	These settings specify the signing certificate used for secure SSO authentication between the Privileged Access Service and the web application. Just be sure to use a matching certificate both in the application settings in the Admin Portal and in the application itself. Select an option to change the signing certificate. Use the Default Tenant Application Certificate (default) Select this option to use the Privileged Access Service standard certificate. This is the default setting. Click Download to save the certificate so you can use it during the application configuration process. If you replace the certificate, be sure to update application with the new certificate information. -Upload New Signing Certificate- Select this option to upload your organization's own certificate. To use your own certificate, you must enter a name and a password (if the file requires a password) and then click Browse to upload an archive file (.p12 or .pfx extension) that contains the certificate along with its private key. Upload the certificate from your local storage prior to downloading any IdP metadata. If the IdP metadata is available from a URL, be sure to upload the certificate prior to providing the URL to your service provider.
Single Sign On URL	The URL that the service provider uses to notify the Privileged Access Service of SAML Single Sign On.

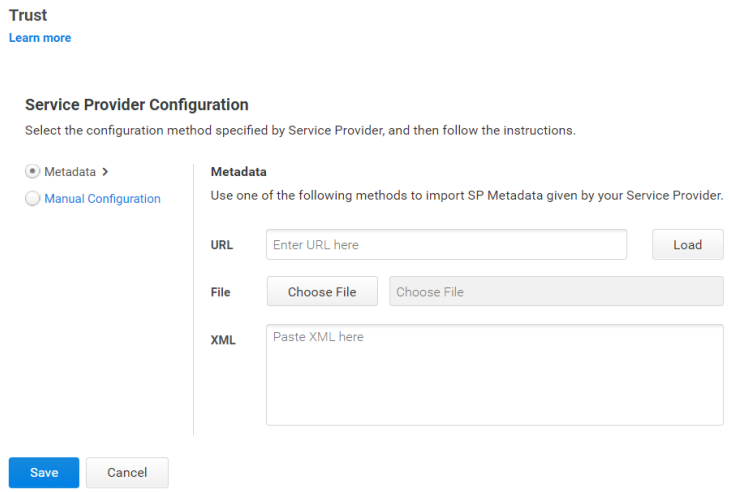
Option	Description
Single Logout URL	The URL the service provider uses to notify the IdP of SAML Single Logout.
Single Sign On Error URL	The URL that the service provider uses to notify the Privileged Access Service if there's a SAML Single Sign On Error.



8. Complete the information for the Service Provider Configuration section by uploading metadata provider by your service provider or by using the manual configuration, then click **Save**.

Description of Service Provider Configuration Metadata fields

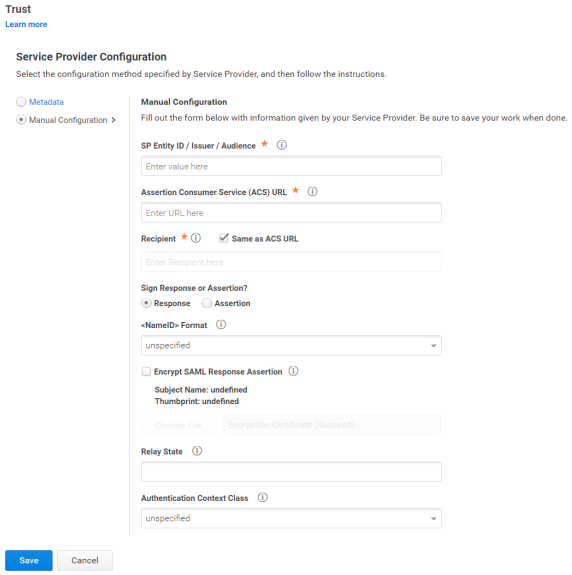
Option	Description
Service Provider Configuration	
Metadata (selected)	
URL	If your SAML application vendor supplies you with an SP Metadata URL, enter the URL in the input field and then click Load.
File	If your SAML application vendor supplies you with an SP Metadata File, click Choose File, select the file. The file name appears in the Choose File field.
XML	If your SAML application vendor supplies you with SP Metadata XML content, copy it and place it in the Paste XML here input field.



Description of Service Provider Configuration Manual Configuration fields

Option	Description
Service Provider Configuration	
Manual Configuration (selected)	
SP Entity ID/ Issuer /Audience	Enter the Entity ID that your SAML application vendor supplies. This Entity ID is also known as Service Provider Issuer or Audience.
Assertion Consumer Service (ACS) URL	The Assertion Consumer Service (ACS) URL specifies the URL to which the Privileged Access Service sends the SAML response. The ACS URL is provided by the application vendor (service provider). Enter the ACS URL provided by the application vendor.
Recipient Same as ACS URL	Only uncheck the checkbox and enter the Recipient value when the Service Provider instructs you to do so.
<NameID> Format	The Service Provider will specify the NameID format to use. If unknown, leave the format as unspecified.
Encrypt SAML Response Assertion	If a Service Provider supports this feature, and you want to use it, check the check box first. Click the Choose File button to select the Public Certificate that the Service Provider sends to you. The Subject Name and Thumbprint information is shown after the Public Certificate has been selected.

Option	Description
Relay State	If the Service Provider specifies a Relay State to use, enter it in the input field.
Authentication Context Class	If the Service Provider specifies the Authentication Context Class to use, select the applicable option. If unknown, leave the option as unspecified.



9. Click **Save** to preserve your changes.
10. On the **SAML Response** page, use the Attributes section to "Configure the SAML Attributes" according to the Service Provider requirements.

    In the Custom Logic section, use the "Editing the Assertion Script" if you require more complex logic for attribute mappings for your SAML Response.
11. (Optional) If you want to easily identify your Custom SAML app, customize the **Application Name** and **Logo** fields on the Settings page for your app.

    This alphabetizes your app under the name you give it and provides the visual cue of your custom logo.

Custom OAuth2 Client

OAuth 2.0 is an open-standard framework and specification for authorizing client applications to access online resources. Authorization works by requiring a client to obtain an access token from a server that in turn grants the client access to specific protected resources. The client then sends the access token to the resource whenever it invokes the resource's endpoints.

Privileged Access Service support OAuth 2.0, allowing custom Delinea client applications access to online resources needed by those applications.

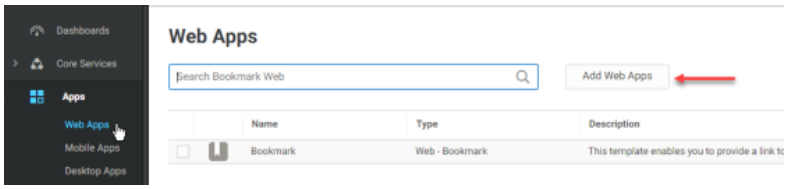
This topic covers how to add the custom OAuth2 Client application to the Admin Portal and describes the available configuration fields and options.

Use the custom OAuth2 Client application if the resulting access token is used to call Privileged Access Service APIs.

Refer to https://developer.delinea.com/docs/oauth for more information about using OAuth 2.0 with Delinea.

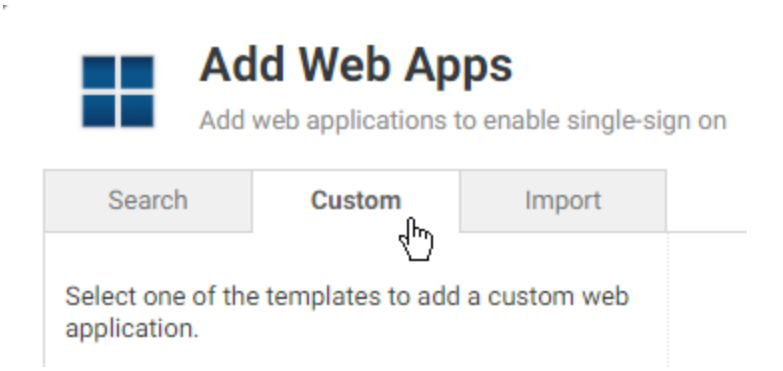
To add and configure a custom OAuth 2.0 client

1. In the Admin Portal, select **Apps > Web Apps**, then click **Add Web Apps**.



   The Add Web Apps screen appears.

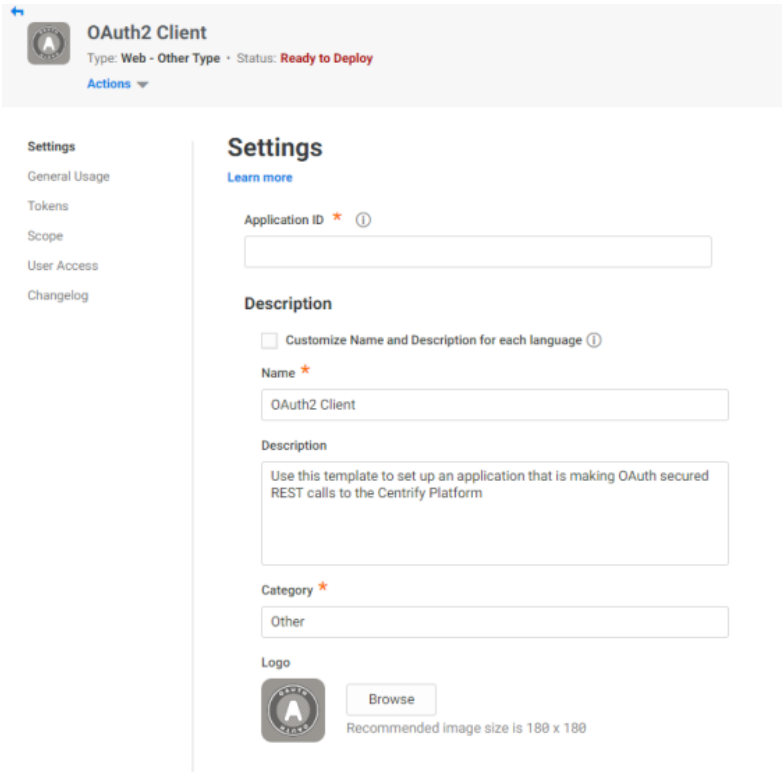
2. Click **Custom**.



3. On the Custom tab, next to the **OAuth2 Client** application, click **Add**.
4. In the Add Web App screen, click **Yes** to add the application.

   The Admin Portal adds the application.
5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Settings page.



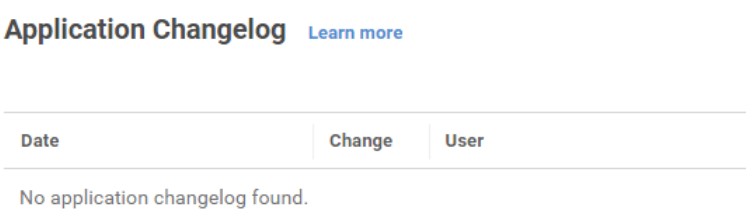
6. On the Settings page, complete the following fields:
   - **Application ID**: a unique key used to build the OAuth2 endpoint URL (URL format is tenant.my.centrify.net/oauth2/introspect/appID.

- **Customize Name and Description for each language**: allows you to specify a name and description for this app, per supported language.
- **Application Name**: a descriptive name for the application.
- **Application Description**: a description for the application.
- **Logo**: you can optionally provide a logo to identify your app.

7. On the **General Usage** page, complete the following fields to specify the types of credentials that can be used to authorize with this server:
   - **Client ID Type:** choose one of these options:
     - **Anything:** allows for authorization in any client where authorization is granted by the user (for example, in a popup screen).
     - **List:** - specifies a list of clients who are allowed access. Click **Add** and then enter the application name of your client.
     - **Confidential:** requires an OAuth2 client to send a client ID and secret. A confidential client is recommended for all flows, but is only required for the Client Credentials flow.
   - **Issuer:** the URL of the server issuing access tokens. Can be left as default.
   - **Allowed Redirects:** specifies the redirects that should be trusted when redirection occurs during the *Authorization Code* and *Implicit* flows. Not applicable for the *Client Credential* and *Resource Owner* flows.
8. On the **Tokens** page, complete the following fields:
   - **Token Type:** specifies the type of token to issue (JwtRS256 or opaque).

     JwtRS256 is a JSON Web Token (JWT) composed of Base64 encoded user and claim information. An opaque token contains no information about the user. To obtain user and claim information for an opaque token an introspection URL must be used by passing the token. The format of the introspection URL is tenant.my.centrify.net/oauth2/introspect/appID .
   - **Auth Methods:** specifies the authentication flow(s) for which the specified token type should be issued.
   - **Token Lifespan:** specifies the token's lifespan.
   - **Issue refresh tokens:** when enabled, allows clients to request a refresh token that can be exchanged for a new access token. Not applicable for the Resource Owner or Client Credentials flows.
9. On the **Scope** page, add any desired scopes and select from the following options:

   Refer to https://developer.delinea.com/docs/client-credentials-flow#step-3-create-scopes for more information about creating scopes.
   - **User must confirm authorization request**: Select this option if you want to the user to confirm the authorization request before receiving a token.
   - **Allow scope selection**: Select this to give users the option of choosing from the scopes that you added.
10. On the **User Access** page, select the role(s) that the user must be in, in order to authorize against the server.
11. (Optional) On the **Changelog** page, you can see recent changes that have been made to the application settings, by date, user, and the type of change that was made.



12. Click **Save**.

Custom OAuth2 Server

OAuth 2.0 is an open-standard framework and specification for authorizing client applications to access online resources. Authorization works by requiring a client to obtain an access token from a server that in turn grants the client access to specific protected resources. The client then sends the access token to the resource whenever it invokes the resource's endpoints.

Privileged Access Service support OAuth 2.0, allowing custom Delinea client applications access to online resources needed by those applications.

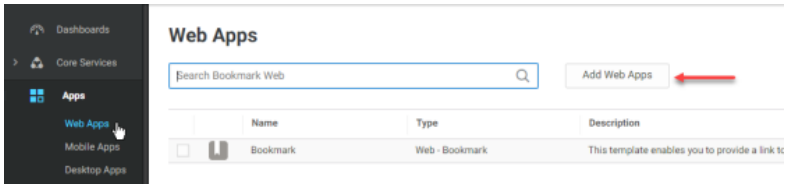
This topic covers how to add the custom OAuth2 Server application to the Admin Portal and describes the available configuration fields and options.

Use the custom OAuth2 Server application for use with another web application's APIs. With the OAuth2 Server application, you can set custom claims in the resulting access token.

Refer to https://developer.delinea.com/docs/oauth for more information about using OAuth 2.0. with Delinea.

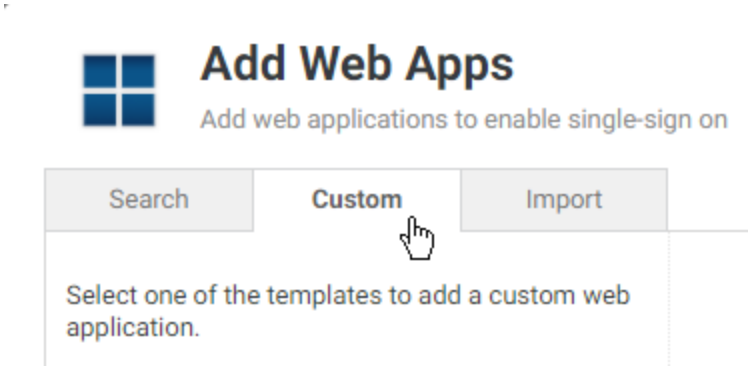
To add and configure a custom OAuth 2.0 Server application

1. In the Admin Portal, select **Apps > Web Apps**, then click **Add Web Apps**.



   The Add Web Apps screen appears.

2. Click **Custom**.

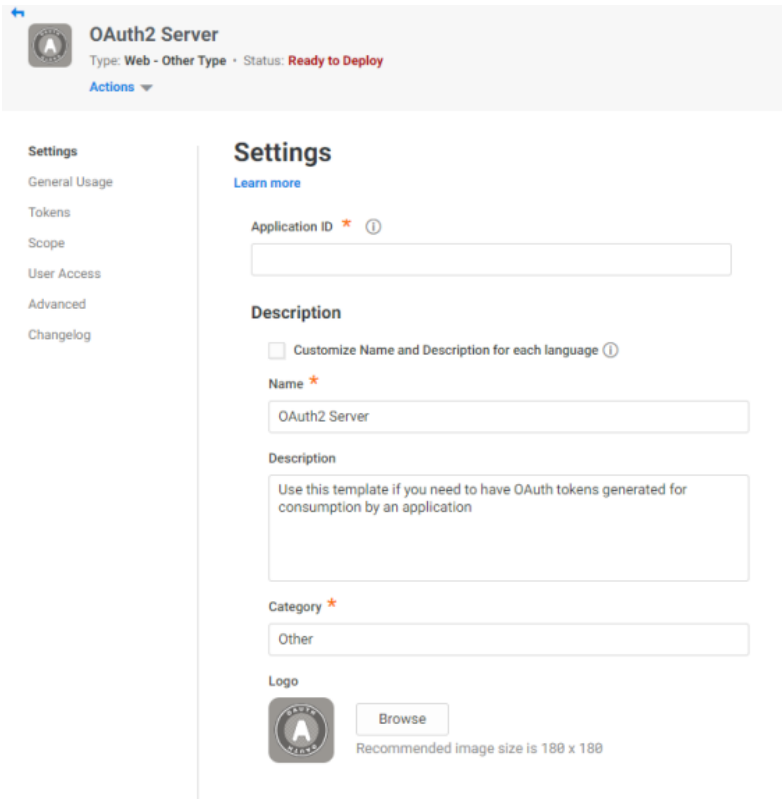


3. On the Custom tab, next to the **OAuth2 Server** application, click **Add**.
4. In the Add Web App screen, click **Yes** to add the application.

   The Admin Portal adds the application.

5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Settings page.

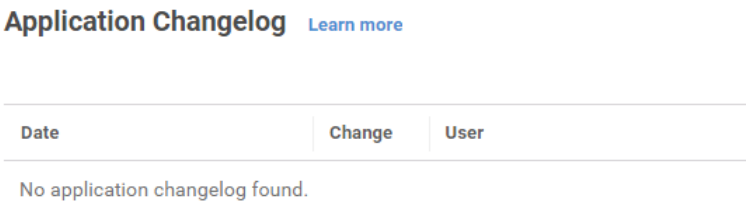


6. On the Settings page, complete the following fields:
   - **Application ID**: a unique key used to build the OAuth2 endpoint URL (URL format is tenant.my.centrify.net/oauth2/introspect/appID.
   - **Customize Name and Description for each language**: allows you to specify a name and description for this app, per supported language.
   - **Application Name**: a descriptive name for the application.
   - **Application Description**: a description for the application.
   - **Logo**: you can optionally provide a logo to identify your app.
7. On the **General Usage** page, complete the following fields to specify the types of credentials that can be used to authorize with this server:
   - **Client ID Type:** choose one of these options:
     - **Anything:** allows for authorization in any client where authorization is granted by the user (for example, in a popup screen).
     - **List:** - specifies a list of clients who are allowed access. Click **Add** and then enter the application name of your client.
     - **Confidential:** requires an OAuth2 client to send a client ID and secret. A confidential client is recommended for all flows, but is only required for the Client Credentials flow.

- **Issuer:** the URL of the server issuing access tokens. Can be left as default.
- **Audience:** metadata that a client may use to verify that the tokens it receives are correct (i.e., allows for client-side verification of a token). Can be set to any string. For example, a client may use this field to ensure a match on the issuer.
- **Allowed Redirects:** specifies the redirects that should be trusted when redirection occurs during the *Authorization Code* and *Implicit* flows. Not applicable for the *Client Credential* and *Resource Owner* flows.

8. On the **Tokens** page, complete the following fields:
   - **Token Type:** specifies the type of token to issue (JwtRS256 or opaque).

     JwtRS256 is a JSON Web Token (JWT) composed of Base64 encoded user and claim information. An opaque token contains no information about the user. To obtain user and claim information for an opaque token an introspection URL must be used by passing the token. The format of the introspection URL is tenant.my.centrify.net/oauth2/introspect/appID .
   - **Auth Methods:** specifies the authentication flow(s) for which the specified token type should be issued.
   - **Token Lifespan:** specifies the token's lifespan.
   - **Issue refresh tokens:** when enabled, allows clients to request a refresh token that can be exchanged for a new access token. Not applicable for the Resource Owner or Client Credentials flows.
9. On the **User Access** page, select the role(s) that the user must be in, in order to authorize against the server.
10. (Optional) On the **Advanced** page, you can enter a custom script that sets claims for JWTs being issued by the tenant for the server.
11. (Optional) On the **Changelog** page, you can see recent changes that have been made to the application settings, by date, user, and the type of change that was made.



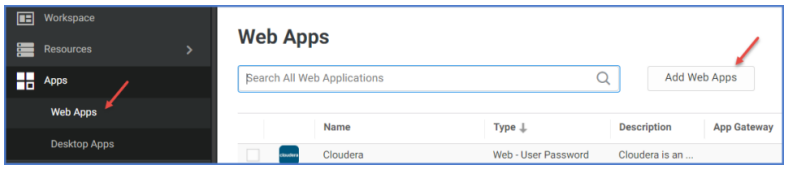
12. Click **Save**.

Adding User-password Applications

Some web applications are configured for user name and password authentication only. Use this option if the application only supports user name and password authentication or if you don't want to configure the application for SAML SSO at this time.

To add and configure a user password application in the Admin Portal

1. In Admin Portal, click **Apps**, then click **Add Web Apps**.



   The Add Web Apps screen appears.

2. On the Search tab, enter the partial or full application name in the Search field and click the search icon.
3. Next to the application, click **Add**.
4. In the Add Web App screen, click **Yes** to confirm.

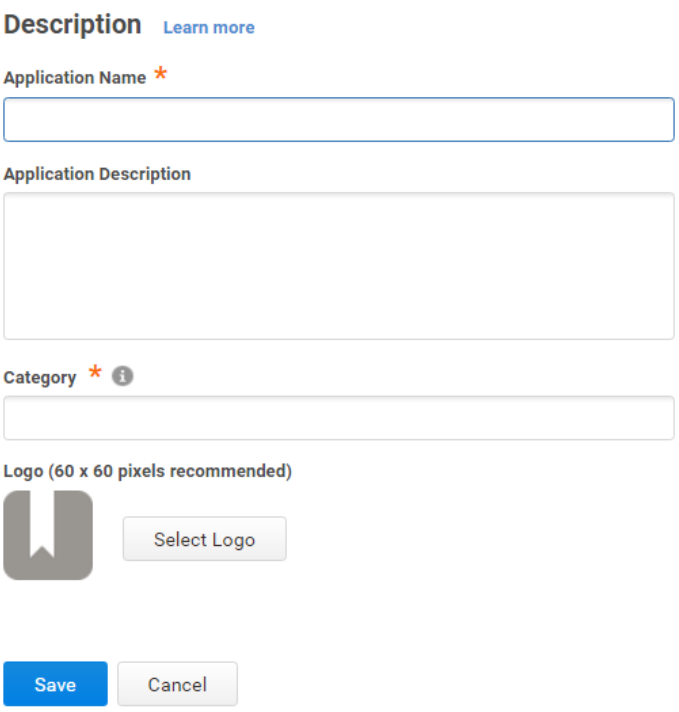
   Admin Portal adds the application.

5. Click **Close** to exit the Application Catalog.

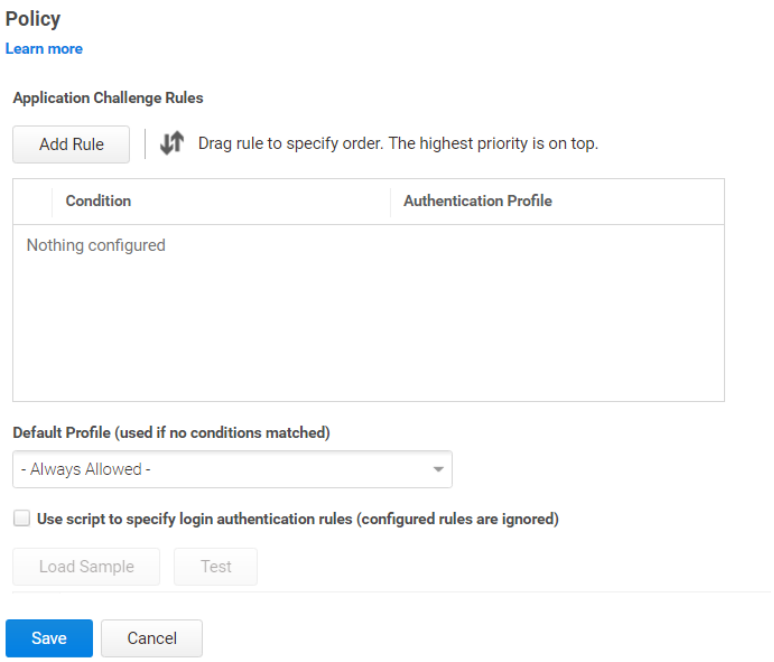
   The application that you just added opens to the Description page.

   Note: The description of how to choose and download a signing certificate in this document might differ slightly from your experience. See "Configuring Single Sign-On (SSO)" on page 838 for the latest information.

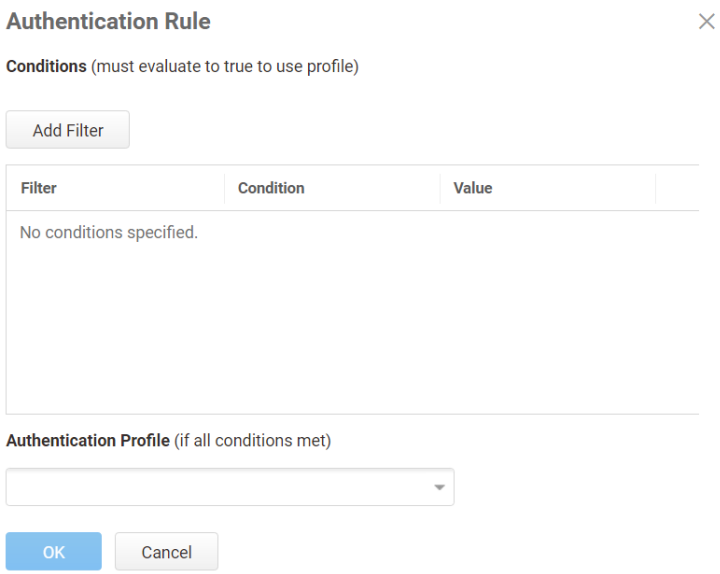
6. (Optional) On the **Description** page, you can change the name, description, and logo for the application. For some applications, the name cannot be modified.



7. (Optional) On the **Policy** page, specify additional authentication controls for this application.



a. Click **Add Rule**.
The Authentication Rule window displays.



b. Click **Add Filter** on the Authentication Rule window.

c. Define the filter and condition using the drop-down boxes.
For example, you can create a rule that requires a specific authentication method when users access the

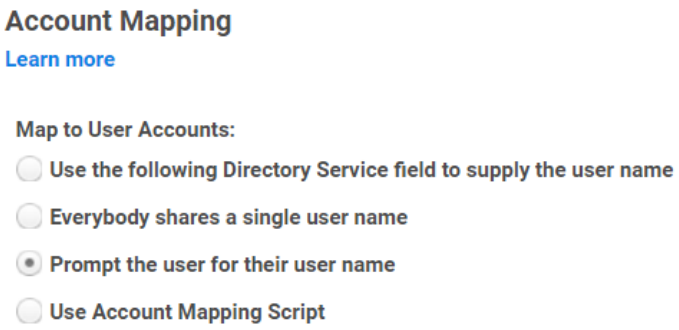
Privileged Access Service from an IP address that is outside of your corporate IP range. Supported filters are:

Filter	Description
IP Address	The authentication factor is the computer's IP address when the user logs in. This option requires that you have configured the IP address range in Settings, Network, Corporate IP Range.
Identity Cookie	The authentication factor is the cookie that is embedded in the current browser by the Privileged Access Service after the user has successfully logged in.
Day of Week	The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.
Date	The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.
Date Range	The authentication factor is a specific date range.
Time Range	The authentication factor is a specific time range in hours and minutes.
Device OS	The authentication factor is the device operating system.
Browser	The authentication factor is the browser used for opening the Privileged Access Service Admin Portal.
Country	The authentication factor is the country based on the IP address of the user computer.
For the Day/Date/Time related conditions, you can choose between the user's local time and Universal Time Coordinated (UTC) time.	

8. Click the **Add** button associated with the filter and condition.
9. Select the profile you want applied if all filters/conditions are met in the **Authentication Profile** drop-down. The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the **Add New Profile** option. See "Creating Authentication Profiles" on page 284
10. Click **OK.**

11. (Optional) In the **Default Profile (used if no conditions matched)** drop-down, you can select a default profile to be applied if a user does not match any of the configured conditions.
    If you have no authentication rules configured and you select **Not Allowed** in the **Default Profile** dropdown, users will not be able to log in to the service.
12. Click **Save**.
    If you have more than one authentication rule, you can prioritize them on the **Policy** page. You can also include JavaScript code to identify specific circumstances when you want to block an application or you want to require additional authentication methods. For details, see "Application Access Policies with JavaScript" on page 987.

    Note: If you left the Apps section of Admin Portal to specify additional authentication control, you will need to return to the Apps section before continuing by clicking **Apps** at the top of the page in Admin Portal.
13. On the **Account Mapping** page, configure how the login information is mapped to the application's user accounts.



The options are as follows:

- **Use the following Directory Service field to supply the user name**: Use this option if the user accounts are based on user attributes. For example, specify an Active Directory field such as *mail* or *userPrincipalName* or a similar field from Delinea Directory.

  For Web - User Password applications, selecting this option allows an additional option to let Active Directory users log in using Active Directory credentials. Select the **Use the login password supplied by the user (Active Directory users only)** option for every Web - User Password application that you want users to log in to using Active Directory credentials.
- **Everybody shares a single user name**: Use this option if you want to share access to an account but not share the user name and password. For example, some people share an application developer account.
- **Prompt the user for their user name**: Use this option if you want users to supply their own user name and password. The first time a user launches the application, they enter their login credentials for that application. The Privileged Access Service stores the user name and password and the next time the user launches the application, the Privileged Access Service logs the user in automatically.

- **Use Account Mapping Script**: You can customize the user account mapping here by supplying a custom JavaScript script. For example, you could use the following line as a script:

  LoginUser.Username = LoginUser.Get('mail')+'.ad';

  The above script instructs the Privileged Access Service to set the login user name to the user's mail attribute value in Active Directory and add '.ad' to the end. So, if the user's mail attribute value is Adele.Darwin@acme.com then the Privileged Access Service uses Adele.Darwin@acme.com.ad. For more information about writing a script to map user accounts, see "User-Password Application Scripting" on page 1024.

14. (Optional) On the **Advanced** page, you can edit the script that provides the login information to the application. In most cases, you don't need to edit this. For details, see "User-Password Application Scripting" on page 1024.
15. (Optional) On the **Changelog** page, you can see recent changes that have been made to the application settings, by date, user, and the type of change that was made.
16. (Optional) Click **Workflow** to set up a request and approval work flow for this application.

    See "Managing Application Access Requests" on page 823 for more information.
17. Click **Save**.

Updating User-password Web Applications

A notification is displayed in the Admin Portal Apps page when updates are available for user-password applications. In general, an application update is prompted when changes are made to the login process for an application. The notification and update procedure are only displayed to users logged in to the Admin Portal with the *sysadmin* role or a role that has *Application Management* permissions.

Note: Updates are only available for user-password applications created by users with the *sysadmin* role or a role that has *Application Management* permission.

To update a web application

1. In the Admin Portal Apps page click **Select apps to receive update** in the notification.

   To dismiss the notification, click the X. A gear icon appears in the upper right section of the Apps page so you can access the Update window after the notification has been dismissed.
2. In the Update window, select the applications that require updating.

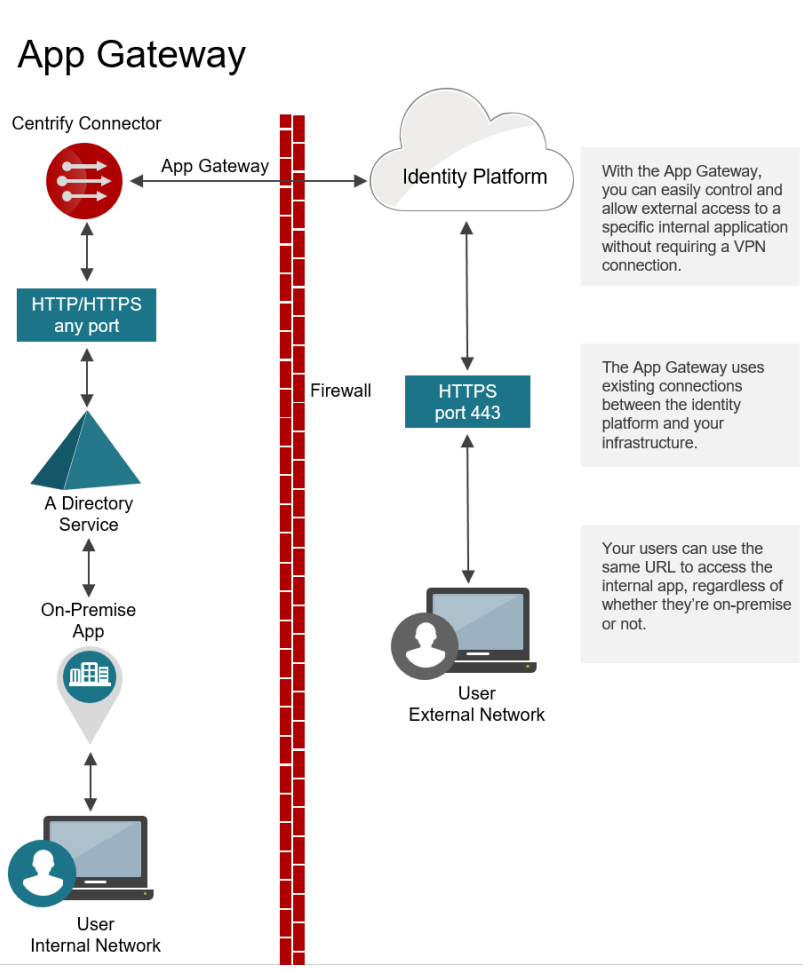
   Note: If do not select to update an application in the list, the old application still works and you can select to do the update later.
3. Click **Update**.

Configuring App Gateway

You can configure on-premise applications so that your users can securely access them outside of your corporate network. Currently, you can require a VPN connection for application access by applying an access policy to the application. VPN connections are relatively straightforward to set up for your entire network, but configuring them to allow or not allow specific applications can be a lot of work. With App Gateway, you can now configure applications for off-site access without requiring a VPN connection.

When users launch an application through a VPN connection, the connection travels an additional pathway. With most VPN connections, the user can access most applications and servers on the corporate network, even if they don't need to do so. If your users need to visit other corporate networks, such as when your sales or other teams visit your customers, your users may not be able to easily launch a VPN connection. And, using VPN connections to access applications off-site can increase the traffic through your VPN tunnel.

For your users, the experience is simple—they enter the application URL and can directly launch the application. In most cases, you'll want to configure the application so that your users can use the same URL to access the application whether they're on the internal network or outside the corporate network.



For applications that use the App Gateway, the connection from the user travels the same network pathways that you already have: the Privileged Access Service connects to the Delinea Connector through the firewall, the Delinea Connector connects to your on-premise directory service, and your on-premise application uses your directory service for authentication and authorization.

For more information on configuring App Gateway, see the following topics:

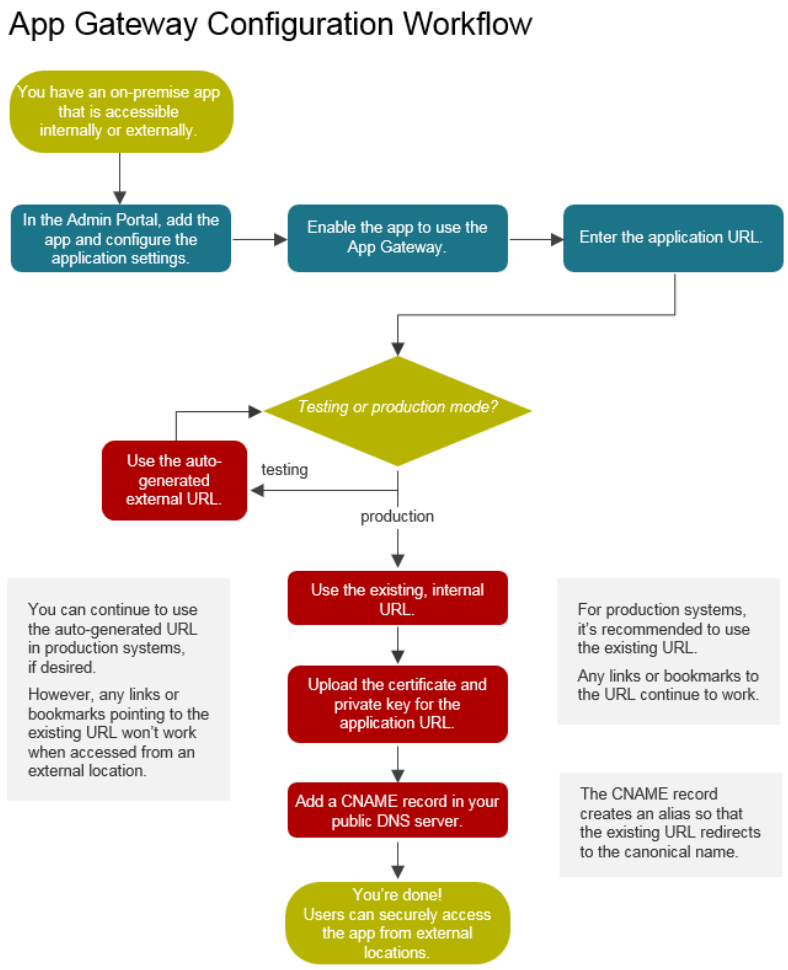
- "App Gateway Configuration Workflow" on page 854.
- "Configuring an Application to Use the App Gateway" on page 855.

- "Adding the CNAME record in your public DNS server" on page 985.
- "App Gateway Troubleshooting" on page 858.
- "Using App Gateway Diagnostics" on page 858.

Content is being migrated. In the meantime please click "Configuring App Gateway" on page 980 for details.

App Gateway Configuration Workflow

Here's an overview of what you need to configure for App Gateway connections:



When you configure an application to use the App Gateway, you don't have to change any configurations in the application directly. In Admin Portal, you enable the application for App Gateway access and you enter the existing URL that users enter to open the application.

At that point, you have a choice: you can use an external URL that the Privileged Access Service automatically generates for you to use, or you can continue using your existing, internal URL. In most cases, it works better for your users to use the auto-generated URL for testing purposes only and then switch over to use the existing URL for external App Gateway access for applications in production mode.

If you use the same DNS name both internally and externally, you must be able to create internal and external DNS entries that point to different things. For example:

Internal zone: Host (A) record pointing to IP address

External zone: CNAME record pointing to <guid>-gw.gateway..centrify.com

Which URL you use involves different advantages and disadvantages.

	Advantages	Disadvantages
Use the App Gateway, and use the auto-generated, external URL for App Gateway connections	Easy to configure and test Excellent for test environments	Existing links and bookmarks won't work outside of the corporate network. Users have to use different URLs depending on whether they're accessing the application internally or externally.
Use your existing, internal URL for App Gateway connections	Existing links and bookmarks work regardless of user login location. Seamless user experience. Recommended for production environments	You do more configuration: you need to upload the URL certificate and private key, and edit your DNS settings.

Configuring an application to use the App Gateway

On the **App Gateway** page, you can configure the application so that your users can access it whether they are logging in from an internal or external location. For applications configured for the App Gateway, users do not have to use a VPN connection to access the application remotely.

Note: App Gateway is an add-on feature. Please contact your sales representative to have the feature enabled for your account.

Note: Some applications can be used with App Gateway; not all applications are set up to use this feature. At this time, Web applications may use HTTPS or HTTP, and either the standard port of 443 or a non-standard port. IP addresses are only supported for on-premise apps and are not supported for external-facing apps.

To configure an application for external App Gateway connections

1. Make sure that your on-premise web application is accessible.

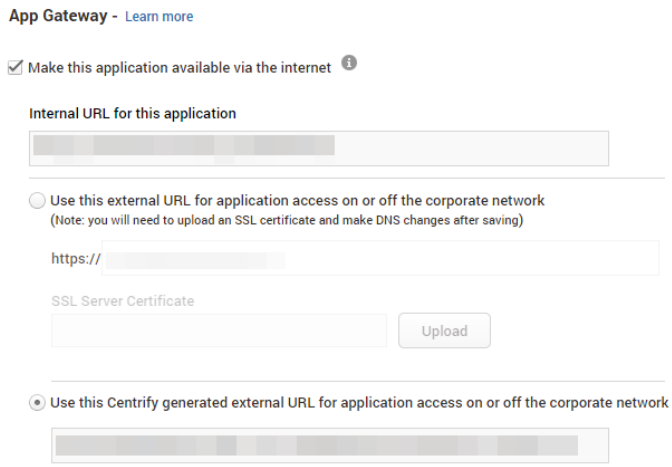
   Note: You can specify a URL that uses either HTTP or HTTPS. To specify the port, add the port at the end of the URL, such as HTTP://acme.log.com:3433. Login URLs with IP addresses are not supported.

2. Install Delinea in your network. If you have already installed them, just make sure that they're the current release version (prior versions don't support App Gateway connections). If you're using a cloud-based directory service, you won't need to install the Active Directory service components with the Delinea Connector.
3. Add, configure, and deploy the application.

   You can enable App gateway access for custom applications, such as user-password and SAML applications.

4. (Optional) On the Application Gateway page, select **Make this application available via the Internet**.

   The Privileged Access Service verifies the application settings and displays the URL that you provided in application settings as the internal URL for the application.



5. Specify the external URL that users open to access the application from external locations. You can use an existing URL or use one that the Centrify automatically generates for you.

   If you use an existing external URL, any links to the application URL do not need to change and will continue to work as is. However, you do need to upload an SSL certificate and modify your DNS settings.

   - To use your existing external URL, select **Use this external URL for application access on or off the corporate network** and do the following:

     a. Enter the existing URL. You can enter an internal or external URL here. Login URLs with IP addresses are not supported.

     b. Click **Upload** to browse to and upload your SSL certificate with the private key for the URL that you entered.

        The certificate file has either a .PFX or .P12 filename extension.

   - To use the auto-generated URL, select **Use this Centrify generated external URL for application access on or off the corporate network**. Later, you'll need to notify users to use the auto-generated URL or access the application from the Admin Portal.

     If you use the auto-generated URL, the option **Rewrite generated external URL to internal URL in requests and responses** found in **Gateway Options** is selected by default to improve compatibility with applications that utilize html redirects in the payload.

6. In **Gateway Options**, select **Lock session to source IP address** to require re-authentication if a user's source IP address changes during the app gateway session.

   This option is not recommended for OWA, as it might cause authentication failures.

7. In **Gateway Options**, select **Lock session to expiration of user** to require re-authentication if a user's identity cookie expires during the app gateway session.

   This option is not recommended for OWA, as it might cause authentication failures.

8. In **Gateway Options**, select **Pass the requested URL to the application without decoding**.

   This option passes the raw URL to the application, which is sometimes necessary for compatibility.

9. In **Gateway Options**, select **Enable standard web proxy headers** to set X-Forwarded-For (RFC-7239), and REMOTE_USER.

   This option allows you to use the App Gateway with network monitoring devices or additional reverse proxies. In addition, you can select either **Client IP Address** or **Username** as values for the X-Forward-For header, depending on whether you want to monitor the header for specific IP ranges or users.

10. Select a connector to use with the application at the __Delinea Connectors to use with this service** section. Choose one of the following:

    - Any available

      Select this option to allow the Privileged Access Service to randomly select one of the available connectors for your App Gateway configuration. Click **Test Connection** to make sure the connection between the connector and the application is successful.

    - Choose

      Select this option to specify one or more Delinea Connectors to use for your App Gateway configuration. If you select more than one connector, the Privileged Access Service randomly chooses one of the selected connectors to use for the application. Once the configuration is saved, each future App Gateway request uses a random connector from those selected, as long as the connector is online.

      Once you select the connectors you want to use, click **Test Connection** to make sure the connection between the selected connectors and the application is successful. At least one connector must succeed in order to save the configuration.

      Note: If any of the Delinea Connectors are offline, they are not displayed in the list of available Delinea Connectors.

11. Click **Save** to save the App Gateway changes.

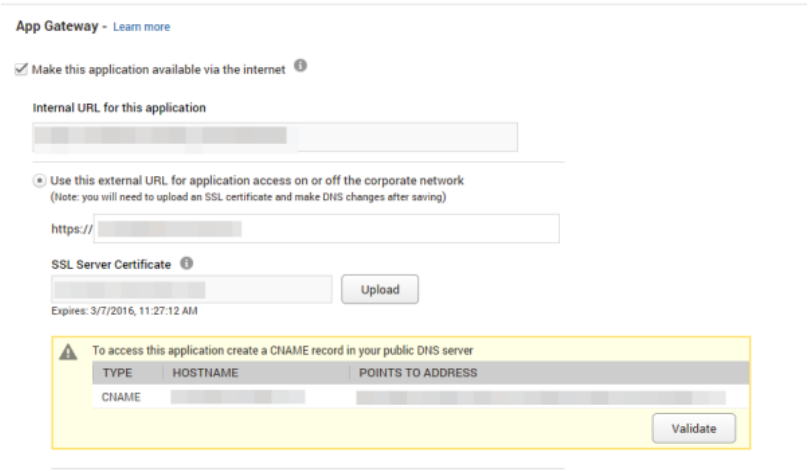
    Note: If you configured the application to use an external URL you need to edit your DNS settings to accommodate the App Gateway connection for this application. For more details, see "Adding the CNAME Record in Your Public DNS Server ".

[priority]: # (4)*

Adding the CNAME record in your public DNS server

When you choose to use your existing external application URL, the Privileged Access Service displays the CNAME record that you need to enter in your public DNS server. This record creates an alias so that when users enter your existing URL (host name), they're redirected automatically to the internal application (by way of the canonical name).

After you upload the certificate, Admin Portal displays the CNAME record entry that you need to enter in your DNS settings.



1. In your domain's DNS settings, you'll enter a CNAME record to map this URL to the application's gateway connection URL.
2. Afterward in the App Gateway settings, you click **Validate** to ensure that the DNS settings are correct.

App Gateway Troubleshooting

Make sure that you have the latest version of the Delinea Connector. See "How to Auto-update Connector Software" on page 421 for more information.

Using App Gateway Diagnostics

App Gateway Diagnostics generates reports that help troubleshoot problems externally accessing applications through App Gateway. App Gateway Diagnostics records web traffic metadata for the application using App Gateway for 24 hours or until you stop the diagnostics session, whichever comes first. Diagnostic reports are generated when you stop the session.

To start a Admin Portal App Gateway Diagnostics session:

1. Configure the application for external App Gateway connections. For more details, see "Configuring App Gateway" on page 852
2. On the **App Gateway** page for the application, click **Start Diagnostics**. A diagnostic sessions starts, indicated by the text **Diagnostic session running ...** .
3. Access the application through the App Gateway as you normally would.

   The diagnostic session records web traffic metadata for the application for 24 hours or until you stop the diagnostics session, whichever comes first.
4. On the **App Gateway** page, click **Stop Diagnostics** to stop the diagnostic session. Links to session reports for the most recent diagnostic session appear.
5. Click the links to view the selected report on the Reports page. The following reports are available.

- Pageloads_<appname><date time>

  The PageLoads report shows page load performance for any page in the application that a user tried to access through App Gateway during the diagnostic session.

- Urls_<appname><date time>

  The Urls report shows absolute links to application content where the hostname differs from the application's tunneled hostname. Any content appearing in this report indicates the application is not compatible with App Gateway. Include this report in any correspondence with Technical Support regarding application compatibility with App Gateway.

  When viewing the report, use the options available in the Actions menu to distribute the reports for use in any correspondence with Technical Support regarding App Gateway connection issues. See Working with reports for more information about the Actions menu.

  Note: All reports generated by App Gateway Diagnostics are available on the **Reports** page in the **Shared Reports > AppGateway** folder. See Managing reports for more information about managing reports.

Scripting

This section provides information on how to use Javascript to more specifically define application access, define and present SAML assertions, define how the Privileged Access Service creates an HTML response for custom user-password applications, define login data to authenticate user sessions for custom Browser extension (advanced) applications, and more.

Working with application scripting

Application Access Policies with JavaScript

If you want to control the circumstances more specifically for which users can access an application or when they need to provide additional authentication credentials, you can use JavaScript. The JavaScript code can determine very specifically when which users are either prevented from accessing an application outside the corporate network or they need to provide additional authentication credentials. You specify the JavaScript in the Policy tab of an application's settings.

It's assumed that you know how to write JavaScript code to use this feature. If you don't know JavaScript, you can use one of the sample scripts that the Privileged Access Service provides. The sample scripts require little to no modification in order to run.

This section includes some guidance as to what types of data that you can specify in your policy script in the following topics. For information about how to use JavaScript, please consult a JavaScript reference guide or tutorial.

- "Data That You Can Use in a Policy Script" on page 996.
- "Entering the Policy Script" on the next page.
- "Using a Sample Policy Script" on the next page.

- "Testing the Policy Script" on the next page.
- "An Advanced Policy Script Example" on page 995.

Entering the Policy Script

You can type directly in the Script field. The policy script screen alerts you to JavaScript syntax errors. You can save a policy script even if there are errors in the code.

Be aware that the script runs frequently, so you'll see better performance if you avoid lengthy and complex calculations.

Using a Sample Policy Script

Admin Portal provides these sample scripts that you can use to indicate specific circumstances for which users cannot launch an application or they need to provide additional authentication details before they can launch the application.

When handling external access, this is defined as users who are logged in from outside of the defined Corporate IP Range (in Settings).

- **Block by AD groups**: This script blocks external access to an application for users in a specific Active Directory group.
- **Block by country**: This script blocks external access to users not in the specified country. The country is determined from the IP address.
- **Block by role**: (requires role specification) This script blocks access to the application for users in a specified role.
- **Block by time**: This script blocks access to the application at all times for users logging in outside of the corporate intranet and allows internal access to the application only during business hours as specified in the policy.
- **Require strong auth for unmanaged devices**: This script determines if the user is logging in from a mobile device that is known about and enrolled in the Privileged Access Service. If the device is not enrolled in the **Privileged Access Service**, the user must supply additional authentication details in order to launch the specified application.
- **Using custom user attributes**: This script defines how a custom user attribute should be used to launch the specified application. For example, you can define that only users where IsFull_TimeEmployee (the custom user attribute) equals true can launch the application.
- **Starter sample**: This script provides an example of what you can do in a policy script.

To use a sample authentication policy script:

1. From the **Apps** page in Admin Portal, open an application and go to the **Policy** tab in the Application Settings dialog box.
2. Click **Load Sample**.
3. Select the desired script and click **Load**.

The sample script displays in the Script field of the Policy tab. You can then test the script to see the results, or simply save the script and other application settings.

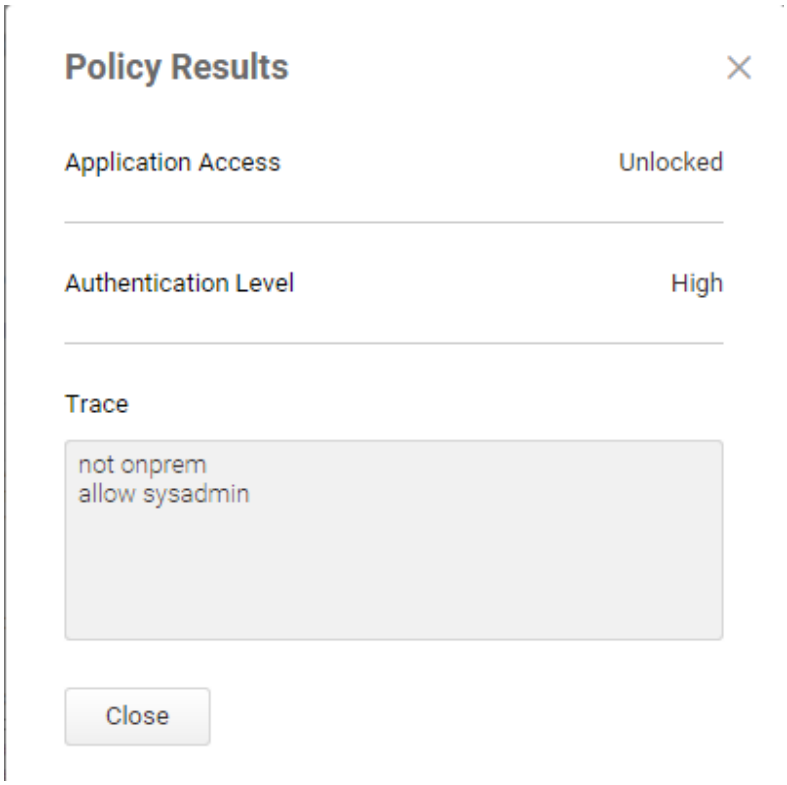
Testing the Policy Script

You can test a policy script to see how it works, based on how you're logged in at the moment. If the script references any user object information, it uses the information from the account you're logged in as.

To test a policy script:

1. From the **Apps** page in Admin Portal, open an application and go to the **Policy** tab in the Application Settings dialog box.
2. Make sure that you've added the JavaScript code for the authentication policy. For example, load the starter script.
3. Click **Test**.

   The Privileged Access Service processes the script and displays the policy results. In the Policy Results dialog box, you can see the application access that is granted and also the authentication level, based on your login information.



   If you've used trace methods in the JavaScript code, the trace results display in the Trace section.
4. Click **Close** to exit the Policy Results dialog box.
5. Either continue working on the policy script, or click **Save** to save your changes and return to the Apps page.

Sample Script Code

Admin Portal provides a few sample scripts that you can use. This section includes the code for those scripts, for your convenience.

Starter Sample Script

```
if(!context.onPrem){
trace("Not onprem");
var umod = module('User');
var user = umod.GetCurrentUser();
if(user.InRole("sysadmin")){
trace("Allow sysadmin");
policy.RequiredLevel = 2;
} else {
trace("Block non-sysadmin");
policy.Locked = true;
}
}
```

Block by Ad Groups Script

```
if(!context.onPrem){
trace("not onprem");
var umod = module('User');
var user = umod.GetCurrentUser();
var blocked_groups = ["\<group_name_1\>", "\<group_name_2\>"];
if (blocked_groups != null)
{
if (user.InEffectiveGroupByNames(blocked_groups)){
trace("block specified AD groups");
policy.Locked = true;
}
}
```

```
}
```

Block by Country Script

```
if(!context.onPrem){
var util = module('Utils');
var country = util.getIpCountryCode(context.ipAddress);
if(country != "US"){
policy.Locked = true;
}
}
```

Block by Role Script

```
if(!context.onPrem){
trace("not onprem");
var umod = module('User');
var user = umod.GetCurrentUser();
var blocked_roles = ["\<role_name_1\>", "\<role_name_2\>"];
if(user.InRoleByNames(blocked_roles)){
trace("block specified role");
policy.Locked = true;
}
}
```

Block by Time Script

```
function toString(n){return (n \< 10? '0' : '') + n;}
function tzOffset(s){
```

```
var i = s.indexOf(":");

return parseInt(s.substring(3, i)) \* 60 + parseInt(s.substring(i+1));

}

// In the line below, replace \<start_day\> with the start of the working day of
the week,

// and \<end_day\> with the end of the working day of the week.

// Example: var workDays = ["1","5"];

var workDays = ["\<start_day\>","\<end_day\>"];

// Replace \<start_time\> with the start of business hours,

// and \<end_time\> with the end of business hours.

// Example: var officeHours = ["08:00:00","17:00:00"];

var officeHours = ["\<start_time\>","\<end_time\>"];

// Replace \<time_zone\> with the office time zone.

// Example: var officeTimeZone = "UTC-08:00";

var officeTimeZone = "\<time_zone\>";

if (workDays[0] == "\<start_day\>" ZZ_BAR_ZZZZ_BAR_ZZ workDays[1] == "\<end_day\>"){

throw "\<start_day\> or \<end_day\> is not set. Please replace \<start_day\> and
 \<end_day\> with the start and end of the working day of the week.";

}

var dayPatt = /\^[0-6]\$/i;

if (!workDays[0].match(dayPatt) ZZ_BAR_ZZZZ_BAR_ZZ !workDays[1].match(dayPatt)){

throw "\<start_day\> or \<end_day\> is not properly set. Please use a number
 between 0 and 6. 0 means Sunday and 6 means Saturday.";

}

if (parseInt(workDays[0]) \> parseInt(workDays[1])){

throw "\<start_day\> or \<end_day\> is not properly set. Please make sure
 \<start_day\> is no later than \<end_day\>.";

}
```

```
if (officeHours[0] == "\<start_time\>" ZZ_BAR_ZZZZ_BAR_ZZ officeHours[1] == "\<end_
time\>"){

throw "\<start_time\> or \<end_time\> is not set. Please replace \<start_time\>
 and \<end_time\> with the start and end time of office hours.";

}

var timePatt = /\^([01]?[0-9]\|2[0-3]):[0-5][0-9]:[0-5][0-9]\$/i;

if (!officeHours[0].match(timePatt) ZZ_BAR_ZZZZ_BAR_ZZ !officeHours[1].match(timePatt)){

throw "\<start_time\> or \<end_time\> is not properly set. Please use 24 hour
 time notation 00:00:00 to 23:59:59.";

}

if (Date.parse("1970-01-01T"+officeHours[0]) \> Date.parse("1970-01-01T"+officeHours[1])){

throw "\<start_time\> or \<end_time\> is not properly set. Please make sure
 \<start_time\> is no later than \<end_time\>.";

}

if (officeTimeZone == "\<time_zone\>"){

throw "\<time_zone\> is not set. Please replace \<time_zone\> with the office
 time zone.";

}

var tzPatt = /\^UTC(\\+ZZ_BAR_ZZ\\-)([01]?[0-9]ZZ_BAR_ZZ2[0-3]):[0-5][0-9]\$/i;

if (!officeTimeZone.match(tzPatt)){

throw "\<time_zone\> is not properly set. Please use format UTC-nn:nn or
 UTC+nn:nn where -nn:nn or +nn:nn is the time zone's offset from UTC.";

}

trace("ipaddress: " + context.ipAddress);

if (context.onPrem){

trace("onprem");

var d = new Date();

d.setMinutes(d.getMinutes() + d.getTimezoneOffset() + tzOffset(officeTimeZone));

var curTime = d.getTime();

var curDay = d.getDay();
```

```
trace("current time: " + d.toLocaleString());

trace("curDay: " + curDay);

if (curDay \< parseInt(workDays[0]) ZZ_BAR_ZZZZ_BAR_ZZ curDay \> parseInt(workDays[1])){

trace("block access - current day is not a working day.");

policy.Locked = true;

return;

}

var dateString = d.getFullYear() + '-' + toString(d.getMonth() + 1) + '-' + toString
(d.getDate());

var startTime = Date.parse(dateString + 'T' + officeHours[0]);

trace("start time: " + dateString + 'T' + officeHours[0]);

var endTime = Date.parse(dateString + 'T' + officeHours[1]);

trace("end time: " + dateString + 'T' + officeHours[1]);

trace("curTime: " + curTime);

trace("startTime: " + startTime);

trace("endTime: " + endTime);

if (curTime \< startTime ZZ_BAR_ZZZZ_BAR_ZZ curTime \> endTime){

trace("block access - current time is not within office hours.");

policy.Locked = true;

}

}

else {

trace("off premises");

trace("block access - user is currently not on premise.");

policy.Locked = true;

}
```

Require Strong Authentication for Unmanaged Devices Script

```
var dmod = module('Device');

var device = dmod.getDevice();

if(!device.isManaged){

policy.RequiredLevel = 2;

}
```

Using Custom User Attributes

In the sample script below, we are defining that only users where IsFull_TimeEmployee (the custom user attribute) equals true can launch the application.

```
var um = module("User");

var u = um.GetUserData(null);

var IsFull_TimeEmployee = u.IsFull_TimeEmployee;

policy.Locked = true;

if(IsFull_TimeEmployee){

trace("userisfulltime");

policy.Locked = false;

}
```

An Advanced Policy Script Example

Here is another sample script; this script extends the starter script example and uses the User and SQL Query modules to allow access only to users who are in a role that starts with k. Although this may not be a practical example, it demonstrates the full power of policy scripting.

```
if(!context.onPrem){

trace("not onprem");

var umod = module('User');

var user = umod.GetCurrentUser();

trace (user.Username);
```

```
trace (user.DisplayName);

trace (user.Properties.Get('mail'));

var sqlMod = module('SqlQuery');

var roles = sqlMod.query('select \* from role where ID like "k_%"');

var inkrole = false;

for(var i = 0; i \< roles.length; i++ )

{

var krole = roles[i].ID;

if(user.InRole(krole)){

inkrole = true;

break;

}

}

if(!inkrole){

trace("block specified role");

policy.Locked = true;

}

}
```

Data That You Can Use in a Policy Script

The policy script operates in addition to the regular authentication options, Intranet Only and Require Strong Authentication. Either the script or these options can determine that an application is blocked or that stronger authentication is needed.

You can reference three kinds of data in a policy script to determine whether a user can access an application or if the user needs to provide more authentication credentials.

- **Application**: You specify an attribute of the application to indicate which application you're referring to. For example, to use the type of web application, you'd use `application.Get("WebAppType")`. When referring to an application, you use a get function for the same attributes that are columns in the Application table. You can see these columns in the Data Dictionary, which is available in the Reports page when building a report.

- **Context**: You can use the context from which the user is accessing the application, such as whether they're in the corporate intranet, the user's IP address, or when the user was last authenticated by the Privileged Access Service.
- **Client**: You can use some attributes of the browser client, such as operating system and browser type.

You can also invoke modules, to access information specific to that module. For example, you can invoke the User module, which allows you to reference user attributes such as the user name or if the user is in a particular role.

You can pass certain data to the script and the script can return whether or not the application access is granted or if authentication is required or not.

> The policy script runs whenever a user tries to launch the application or whenever the Admin Portal refreshes

Application Context Variables to Use

You can use any of the following application contexts in your policy script:

- **context.lastAuthenticated**: This specifies the date and time when the user was last authenticated by the Privileged Access Service. This can either refer to the last time that the user entered their user name and password, or the last time that they were automatically logged in by way of IWA. You can also call `context.lastAuthenticated.ToString()` to convert the returned date and time to a string value.
- **context.authLevel**: This specifies the current authentication level. If the user has used regular authentication (no additional or Strong Authentication methods), the authentication level is 1. Level 2 is Strong Authentication.

- **context.onPrem**: This specifies whether the user is currently logging in from inside the corporate intranet (as specified in the Corporate IP Range settings). This variable returns a boolean value. If you haven't specified a Corporate IP Range, this context.onPrem is always false.
- **context.ipAddress**: This specifies the user's current IP address that is visible to the internet. If a user is logged in on your internal network, keep in the mind that the IP address is the address of the web proxy or NAT gateway.

Client Examples

You can use the following client information:

- **client.oS**: This specifies the user's operating system.
- **client.application**: This specifies the thick applications that the Privileged Access Service is aware of, such as Outlook, Lync, and so forth.
- **client.userAgent**: This specifies the browser identity.

Debugging with the Trace Method

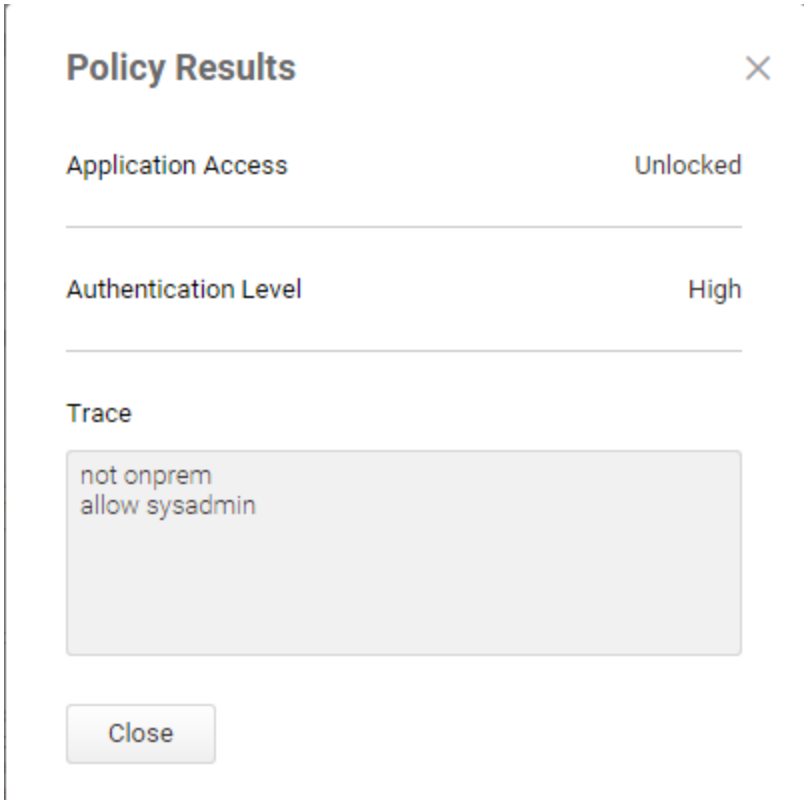
You can use the trace method to debug your policy scripts. With the trace method, you can test your script and see what values are calculated or set.

The trace method takes a single string. The policy script screen logs and displays this string when you click Test. For non-string values, use `toString()`.

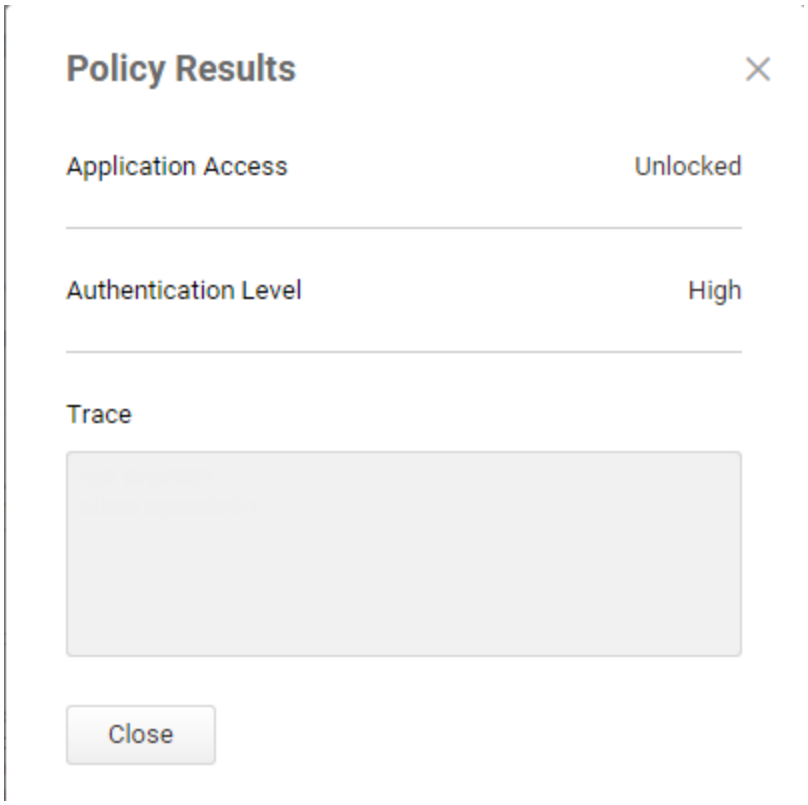
For example, the starter script uses the trace method a couple of times:

```
if(!context.onPrem){

trace("not onprem");

var umod = module('User');

var user = umod.GetCurrentUser();

if(user.InRole("sysadmin")){

trace("allow sysadmin");

policy.RequiredLevel = 2;

} else {

trace("block non sysadim");

policy.Locked = true;

}

}
```

For example, if you run this script as a member of the sysadmin role and you haven't specified the Corporate IP range, you see the following result:



If you're within the corporate intranet, you see no trace results because the starter script mainly handles situations where the user is not logged in to the corporate intranet.



Specifying the Policy Result

To specify the policy result, you set attributes on the policy object. The options are as follows:

- `policy.Locked` (true or false)
- `policy.Reason` (“Your custom message.”)
- `policy.RequiredLevel` (1=normal, 2=strong authentication)

For example, if you want to force strong authentication, you set the `policy.RequiredLevel=2`. If you want to block access to the application, you set the `policy.Locked = true`. If `policy.Reason` is not specified, the default value is “Application is not currently available” and the user will see this message when launching the app.

The sample starter script uses `policy.Locked` and `policy.RequiredLevel`, but does not specify a `policy.Reason`.

Modules

Admin Portal provides JavaScript modules that you can use in your policy script. These modules provide libraries of functions related to different kinds of data. To use any of the functions that are in a module, be sure to invoke the module first.

For example, the starter script invokes the user module:

```
if(!context.onPrem){
```

```
trace("not onprem");

var umod = module('User');

var user = umod.GetCurrentUser();

if(user.InRole("sysadmin")){

trace("allow sysadmin");

policy.RequiredLevel = 2;

} else {

trace("block non sysadim");

policy.Locked = true;

}

}
```

SqlQuery Module

The SqlQuery module allows you to perform SQL queries from within the policy script. You can query the same tables and columns that you use in a report query.

You can use the following methods from the SqlQuery module:

query('*sql query statement*'): runs a SQL query.

For more information about SQL queries against data, see "Managing Reports" on page 1053.

Utils Module

You can use the following functions from the Utils module:

- `getIPLocation(*IPAaddress*)`: returns an object with the following geographical properties: city, countryCode, countryName, latitude, longitude.
- `getGeoDistance(*alat,blat,along,blong*)`: returns the distance between two locations, in kilometers.

SAML Application Scripting

You can use the SAML application template to add a SAML-enabled web application to the app catalog. This template creates a SAML application profile for a web application that defines how the Privileged Access Service presents an authenticated user to the web application via a SAML assertion.

Each SAML application profile requires a custom SAML script. The script defines how the Privileged Access Service creates and presents a SAML assertion for each user's session with the web application. Each application profile may also provide an optional user map script that determines the user's application log-on name for use in the SAML assertion. Both scripts are written in JavaScript.

This guide provides these sections:

- "SAML Authentication Overview" below is an overview of the SAML authentication process for a user session with a web application. It shows how the Privileged Access Service works with a set of JavaScript objects during the process.
- "Writing a User Map Script" on page 1004 describes how to write an optional user map script to specify an application user log-on name for a user session.
- "Writing a Custom SAML Script" on page 1006 describes how to write the required custom SAML script to define a SAML assertion for a user session.
- "Scripting Environment Reference" on page 1016 is a reference section for the objects, methods, and variables in the user map and SAML scripting environment.

To write a SAML script, you need to know how to write code in JavaScript. You also need to know the basics of SAML authentication to understand how to specify a SAML assertion. This guide provides some guidance about SAML configuration values, but for specifics you can consult the SAML specifications. For an introduction to SAML, try the overview section of the SAML documentation.

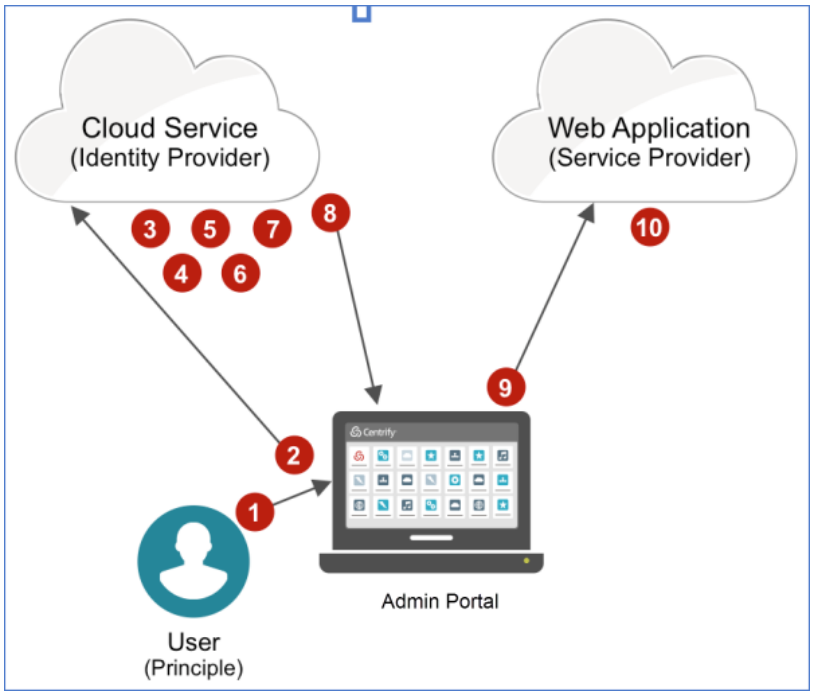
SAML Authentication Overview

When a user asks to connect to a SAML-enabled web application in the Admin Portal, the traditional SAML roles are these:

- The **principal** is the user, who's already been authenticated in the Admin Portal through the Privileged Access Service. The principal is using a web browser (connected to the Admin Portal) or the mobile application as his user agent to request a web application connection.
- The **identity provider** is the Privileged Access Service, which provides a SAML assertion that presents the user as an authenticated principal.
- The **service provider** is the web application host that receives the SAML assertion and decides whether or not to grant resource access to the principal (the user).

The SAML Authentication Process

When the Privileged Access Service presents a user to a SAML-enabled web application, it creates a SAML assertion for the user session that satisfies the requirements of the service provider (the web application host) and presents necessary information about the current user. The following figure shows the steps the Privileged Access Service takes when it authenticates a user to a SAML application added to the app catalog using the generic SAML application template. The steps follow.



1. The user launches the web application in the Admin Portal.
2. The Admin Portal notifies the Privileged Access Service that the user wants a session with the web application.
3. The Privileged Access Service creates a set of JavaScript objects for this SAML user session:
   - An **Application object** that contains the properties of the web application as they're defined in the web application profile. Those properties are defined using the generic SAML application template and include the application name, the URL, the issuer, the IdP sign-in URL, and others that appear in the template in the Admin Portal. The Application object is a read-only object. A script reads its properties through the object's Get() method.
   - A **LoginUser object** that contains information about the user identity used to log onto the service provider: the user identity recognized by the web application (which is not necessarily the Admin Portal login user name) and so on. This is a read-write object that the Privileged Access Service or the user map script may alter before it's used later in the custom SAML script to set the user name in the SAML assertion.
   - A **private assertion object** that defines the elements of the SAML assertion that the Privileged Access Service builds to send to the web application. This object isn't visible to the custom SAML script, but the script may set the assertion object's properties using a family of global "set" methods (described later).
4. The Privileged Access Service determines the web application log-on user name as it was specified in the generic SAML application template. The template specifies one of these three methods:
   - The Privileged Access Service checks the user's Active Directory user record through the connector, retrieves the specified attribute as the application user name, then assigns the user name to the LoginUser.Username property. The Privileged Access Service caches the returned attribute so that it doesn't have to retrieve it again from Active Directory for later identical queries.

- The Privileged Access Service reads the shared single user name specified in the template and assigns it to `LoginUser.Username`.
- The Privileged Access Service executes the user map script set in the template, which creates a user name and assigns it to `LoginUser.Username`.

5. The Privileged Access Service executes the custom SAML script to specify a SAML assertion for the user session.

   The script must define all the SAML assertion elements required by the web application. The script uses the global assertion-set methods to define the elements in the private assertion object.
6. The Privileged Access Service creates a SAML assertion based on the properties of the private assertion object and includes the assertion in a SAML response.
7. The Privileged Access Service signs the SAML response (or the SAML assertion within the response, depending on what's specified in the custom SAML script). It uses the Privileged Access Service certificate private key unless the application profile is set to provide a different certificate. (Certificate assignment is set in the Application Settings tab of the generic SAML application template.)
8. The Privileged Access Service sends the SAML response to the Admin Portal (or the browser running it). The SAML response has a redirection that instructs the Admin Portal to send the response to the web application at the URL specified in the SAML assertion.
9. The Admin Portal sends the SAML response to the specified URL.
10. The web application reads the SAML response and then (if the key and assertion checks out) logs the user into the web application.

Writing a User Map Script

The user map script is JavaScript that you may set up as an optional way to determine the user name used to log onto a web application.

Entering a User Map Script

To enter the user map script in the Application Settings tab of the generic SAML application template:

1. Under **Account Mapping**, select **Use Account Mapping Script** to open the user map script text panel.
2. Enter the script in the text panel.

   Incorrect JavaScript syntax in a line triggers a yellow symbol before the line number.
3. (Optional) Click **Test**.

   The Test Results window opens showing Account Mapping Details and the results of a Trace of the script. The Account Mapping Details list displays the attributes of the mapped `LoginUser`.
4. Click **Save Changes**.

Read "To Add and Configure a Custom SAML Application" on page 962 for more information about using the generic SAML application template.

User Map Script Elements

The user map script is an optional way to determine the user name to present to a web application if the other user mapping options won't provide what's required. Your script can examine current application and user properties for this user session and can use that information and any other factors to create a user name. The user map script must, at some point, assign a user name to the `LoginUser.Username` property, where it's retrieved later to create a SAML assertion.

An Example Script

This sample user map script creates a user name by adding the application name to the current user name. The script re-assigns the result back to `LoginUser.Username`.

```
LoginUser.Username = LoginUser.Username + "\#" + Application.Get("Name");
```

When the user's user name is "barney.blanton" wants to log into the web application named "Busfare," the script creates the user name "barney.blanton#Busfare". The script re-assigns this created user name back to `LoginUser.Username`, where the custom SAML script will find the user name later and use it for the SAML assertion.

Retrieving Application Information

If the user map script requires information about the current web application, it can retrieve properties from the Application object created for this user session.

The method `Application.Get()` retrieves those properties. It takes as its argument a string that specifies the property whose value to retrieve. `Application"Name"`, for example, retrieves the name of the application.

"Application Object" on page 1017 describes all of the Application object's properties that you may retrieve. These properties aren't typically used for determining a user name, although the application name may sometimes be useful.

Retrieving LoginUser Properties

If the user map script requires information about the current user settings, it can examine the properties of the `LoginUser` object created for this user session. "LoginUser Object" on page 1019 describes the `LoginUser` properties.

Several of these properties (`LoginUser.GroupNames`, for example) contain an array of group names of which the user is a member. These might be useful, depending on your requirements, for determining a user name. You might, for example, specify a single user name for anyone belonging to the admin group, and specify another single user name for anyone belonging to the sales group.

You can also use the `LoginUser.ServiceName` and `LoginUser.ServiceType` properties to distinguish between directory sources. For example, if the user is managed by Active Directory, some attributes might be different than users managed by LDAP (`userprincipalname` for AD and `UID` for LDAP). Use either of these properties to determine the user's directory source.

Retrieving the User's Directory Attributes

The `LoginUser` object offers a single method, `Get()`, that retrieves any one of the current user's attributes. It takes as its argument a string that specifies the key of the attribute to retrieve. `LoginUser.Get("mail")`, for example,

returns the user's email address as stored in Active Directory.

When `LoginUser.Get()` executes, the Privileged Access Service contacts the source directory through the connector for the user's organization and retrieves the attribute. If, for example, an Active Directory user has logged into the Admin Portal as a member of the Acme organization, executing `LoginUser.Get()` during one of that user's log-on sessions contacts the Acme Active Directory service through the connector set up in Acme's internal network. If a Privileged Access Service user has logged in, executing `LoginUser.Get()` queries the Cloud Directory Service (CDS).

> Not all attributes are common between directory services. If you have uses managed by different directory services (for example, AD and LDAP), use the `LoginUser.ServiceType` or `Login.User.ServiceName` properties to determine the user's source directory and then get the appropriate attribute key. Refer to "LoginUser Object" on page 1019 for more information.

Example

```
if(LoginUser.ServiceType == 'LDAPProxy'){

UserIdentifier = LoginUser.Get('uid');

} else {

UserIdentifier = LoginUser.Username;

}
```

Explanation

The preceding example checks to see if the user is managed by LDAP. If the user's service type is LDAPProxy, the script gets the current user's UID attribute, otherwise it uses the `LoginUser.Username` property.

Specifying the User Logon Name

Once your script has created a web application log-on name as a string value, it must assign it to the `LoginUser.Username` property. The script can assign the user name string directly to the property.

Writing a Custom SAML Script

You can write SAML response scripts in JavaScript in the Custom Logic area of the SAML Response page of a SAML application.

The custom SAML script specifies elements that must be present in the SAML assertion used to start the current user session with a web application. To write the script, you must know what SAML elements the web application requires. The script must retrieve required information from the web application's profile and the user object, and must then specify the SAML elements and their values using assertion-set methods. After the script executes, the Privileged Access Service follows the script's specifications to create a SAML assertion and its enclosing SAML response.

A SAML script is required for each application profile created using the custom SAML application template. To see examples of SAML scripts used to connect to web services, open the application profile for any SAML application in the Apps panel of Admin Portal. Click the **SAML Response** tab to see the application's SAML script.

To assist with writing SAML response scripts, the SAML Script Editor includes a context-sensitive autocomplete feature.

Determining SAML requirements for the web application

Each SAML web application typically requires its own set of SAML elements in a SAML assertion. Although many of the elements will be the same from application to application, there are enough variations that one script won't cover all applications.

To write a script for a SAML web application, you must find out from the application's publishers what its SAML requirements are. If the application is a large public application, its publishers may present their SAML requirements on their web site. As an example, Salesforce publishes SAML requirements for authentication here. Most large public SAML web applications, however, will probably already be in the app catalog so you won't need to add them via the generic SAML application template.

For web applications that don't provide their SAML requirements publicly, you'll have to contact technical support or their development team to ask about their SAML requirements. This requires some familiarity with SAML. Reading through a public SAML application's SAML requirements (such as Salesforce's requirements) is a good start to understanding what a typical SAML application requires.

Retrieving information

The custom SAML script has access to the same JavaScript objects, global methods, and global variables that the user map script has along with some additional application-set methods used to specify SAML elements. To retrieve application and user information, use the Application and LoginUser objects that the Privileged Access Service creates for a user session.

Application object

The Privileged Access Service creates a single `Application` object for each SAML user session. The object is an instance of the `ReadOnlyDataEntity` class, and is a read-only object.

The `Application` object's properties describe the SAML web application as it's defined in the application profile. Create a SAML web application profile in the Admin Portal using the customSAML application template (described in "Custom SAML Applications" on page 961.

A script accesses the object's properties using the object's single public function.

Function Name	Description
`Application.Get (*property*)`	This function returns an Application object property. It takes as its argument a string that specifies the property to return. An example: `Application.Get("Name")` returns the name of the application as entered in the Application Settings tab.

The `Application.Get()` function may take the following property names as an argument. Each argument returns a different application property. The property names are case-sensitive.

Property Name	Description
`\_PartitionKey`	The customer ID used to establish the user session. An example: BZ284.
`\_RowKey`	The UUID (universally unique identifier) of the application.
`Description`	The text description of the web application entered in the description field of the Application Settings tab.
`Icon`	The graphic file used as the icon for this application as set in the Application Settings tab.
`Issuer`	The entity ID specified in the Issuer field of the Application Settings tab. Synonymous with the global variable Issuer.
`Name`	The name of the application as entered in the Application Settings tab.
`SamlScript`	The custom SAML script set in the Advanced tab.
`TemplateName`	The type of generic application template used to define this web application's profile. Possible return values: Generic SAML Generic User-Password
`Url`	The contact URL specified in the URL field in the Application Settings tab. Synonymous with the global variable `ServiceUrl`.
`UserName` Strategy	The technique specified in the Application Settings tab to determine the user name (user identity) for a user session. Possible return values: **ADAttribute**: the Privileged Access Service sets the user name to the specified AD attribute of the current user. The Privileged Access Service queries the connector for the AD attribute. The Privileged Access Service caches the user name so that it doesn't have to query the connector for this user's future sessions. **Fixed**: the Privileged Access Service sets the user name to the value entered in the Application Settings tab. **UseScript**: the Privileged Access Service executes the user map script to determine the user name.
WebAppType	The authentication function used by the web application. Possible return values: SAML UsernamePassword

LoginUser object

The Privileged Access Service creates a single LoginUser object for each SAML user session. The object is an instance of the `LoginUser` class, and is a read/write object.

The function `LoginUser.Get()` retrieves any one of the current user's attributes. It takes as its argument a string that specifies the key of the attribute to retrieve. `LoginUser.Get("mail")`, for example, returns the user's email address as stored in Active Directory.

When `LoginUser.Get()` executes, the Privileged Access Service contacts the source directory through the connector for the user's organization and retrieves the attribute. If, for example, an Active Directory user has logged

into the Admin Portal as a member of the Acme organization, executing `LoginUser.Get()` during one of that user's log-on sessions contacts the Acme Active Directory service through the connector set up in Acme's internal network. If a user has logged in, executing `LoginUser.Get()` queries the Cloud Directory Service (CDS).

Note: Not all attributes are common between directory services. If you have uses managed by different directory services (for example, AD and LDAP), use the `LoginUser.ServiceType` or `Login.User.ServiceName` properties to determine the user's source directory and then get the appropriate attribute key. Refer to "LoginUser Object" on page 1019 for more information.

Example

```
if(LoginUser.ServiceType == 'LDAPProxy'){

UserIdentifier = LoginUser.Get('uid');

} else {

UserIdentifier = LoginUser.Username;

}
```

Explanation

The preceding example checks to see if the user is managed by LDAP. If the user's service type is LDAPProxy, the script gets the current user's UID attribute, otherwise it uses the `LoginUser.Username` property.

The `LoginUser` object has the following methods:

Function name	Description
`LoginUser.Get(ADkey)`	This function returns any one of the current user's Active Directory attributes. It takes as its argument a string that specifies the key of the attribute to retrieve. An example: `LoginUser.Get("mail")` returns the user's email address as stored in the user's Active Directory account.
`LoginUser.GetValues(ADkey)`	This function returns an array with all values of an Active Directory attribute with multiple values for the current user. It takes as its argument a string that specifies the key of the attribute to retrieve. For example, the line `setAttributeArray('proxies', LoginUser.GetValues('proxyAddresses'));` sets an attribute array named proxies that includes all values for the logged in user for the AD key proxyAddresses.

Function name	Description
`LoginUser.GetGroupAttributeValues (ADkey)`	This function returns the values of the current user's groups specified AD attribute. It takes as its argument a string that specifies the key of the attribute to retrieve. An example: `LoginUser.GetGroupAttributeValues("sAMAccountName")` returns the user's groups `sAMAccountName` value as stored in the user's Active Directory account.

The `LoginUser` object's properties describe the user as he or she is presented to the web application. The following table describes those properties.

Property name	Description
`LoginUser.Username`	The user identity presented in the SAML assertion to the web application. The Privileged Access Service determines the user ID for this user session depending on the "Map to User Accounts" setting in the Application Settings tab. (These settings determine the user name, which is the user ID presented in the SAML assertion.)
`LoginUser.FirstName`	The first name of the user presented in the SAML assertion to the web application. Note the following special cases for parsing this attribute for users in directory services that do not have the `FirstName` attribute, such as Delinea Directory: `FirstName` attribute is parsed from the first string of `DisplayName`. If `DisplayName` is a single string, the same string is used for the `FirstName` and `LastName` attributes. If `DisplayName` is null, `FirstName` and `LastName` return as null. SAML apps that require non-empty values will fail to launch in this case.
`LoginUser.LastName`	The last name of the user presented in the SAML assertion to the web application. Note the following special cases for parsing this attribute for users in directory services that do not have the `LastName` attribute, such as Centrify Directory: The `LastName` attribute is parsed from the last string of `DisplayName`. Any additional strings between the first string and the last string are ignored. If `DisplayName` is a single string, the same string is used for the `FirstName` and `LastName` attributes. If `DisplayName` is null, `FirstName` and `LastName` return as null. SAML apps that require non-empty values will fail to launch in this case.
`LoginUser.GroupNames`	An array of group names for groups in which the user is an effective member (according to the user's Active Directory account). A user is an effective member of a group if he is either a direct member of the group or is a direct member of a group that is in turn a member of the group. This property returns the same value as `LoginUser.EffectiveGroupNames`.

Property name	Description
`LoginUser.GroupNames2`	An array of group names for groups in which the user is an effective member (according to the user's Active Directory account), returning only the user's group' 'name attribute.
`LoginUser.RoleNames`	An array of Privileged Access Service role names for roles in which the user is a member. The following example illustrates how to set an array named "Groups" that includes the Delinea roles that the logged in user is a member of. `setAttributeArray("Group", LoginUser.RoleNames);`
`LoginUser.EffectiveGroupNames`	An array of group names for groups in which the user is an effective member (according to the user's Active Directory account). A user is an effective member of a group if he is either a direct member of the group or is a direct member of a group that is in turn a member of the group. This property returns the same value as `LoginUser.GroupNames`.
`LoginUser.GroupDNs`	An array of distinguished names of groups in which the user is an effective member. This property returns the same value as `LoginUser.EffectiveGroupDNs`.
`LoginUser.EffectiveGroupDNs`	An array of distinguished names of groups in which the user is an effective member. This property returns the same value as `LoginUser.GroupDNs`.
`LoginUser.ServiceType`	The type of directory service managing the user's user object. Possible values are: ADProxy LDAPProxy CDS (Cloud Directory Service) FDS (Federated Directory Service)
`LoginUser.ServiceName`	The name of the directory service managing the user's user object. These values are set by the network administrator. This property is useful in environments with more than one LDAP proxy.

Specifying SAML assertion elements

The Privileged Access Service offers a group of global assertion-set methods in a user session. These methods set the attributes of the private assertion object, which specifies how the Privileged Access Service will construct the SAML assertion for this user session. Most of these methods take as an argument the value for a specific SAML assertion element. setIssuer(), for example, accepts an entity ID and uses it to specify the issuer URL in the SAML assertion.

Two of the assertion-set methods, `setAttribute()` and `setAttributeArray()`, specify a SAML response attribute by name and then specify a value for that attribute that is either a single argument or an array.

The following table lists the most commonly used assertion-set methods. "Global Methods" on page 1022 describes these methods in full.

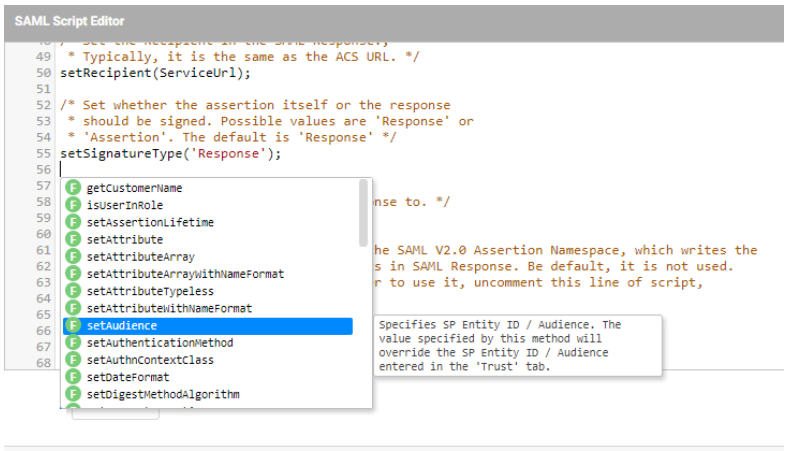
global Function	Description
`setVersion(*samlVersion*)`	Specifies the version of the SAML assertion. “1” specifies version 1.1, “2” specifies version 2.0. The default is 2 if this function isn’t present in the script.
`setIssuer(*issuer*)`	Specifies the issuer in the SAML assertion. Typically a URL provided by retrieving the Application property Issuer or by using the property’s synonymous variable Issuer.
`setSubjectName(*username*)`	Specifies the subject in the SAML assertion, which is the log-on name used for the web application. It’s typically provided by retrieving the `LoginUser.Username` property or by using the property’s synonymous variable `UserIdentifier`. If you have multiple directory sources, use the `LoginUser.ServiceName` or `LoginUser.ServiceType` properties to set an appropriate subject name. For example: `if(LoginUser.ServiceType == 'LDAPProxy'){ setSubjectName(LoginUser.Get('uid')); } else { setSubjectName(LoginUser.Username);}`
`setAudience(*audience*)`	Specifies the audience in an audience restriction in the SAML assertion. This typically takes the entityIDURL such as “https://login/myapp.com".
`setRecipient(*recipient*)`	Specifies the recipient in the SAML assertion’s `SubjectConfirmationData` element. This typically takes the ACS/entityID URL such as "https://login/myapp.com”.
`setSignatureType (*signingPref*)`	Specifies whether the SAML assertion should be signed, or the SAML response that contains the assertion. The two possible values are “Response” or “Assertion”. The default is “Response” if this function isn’t present in the script.
`setServiceUrl(*targetUrl*)`	Specifies the value for the `TARGET` form element (the resource requested for the user session) when posting the SAML response. This is typically a URL that is the same as that used for the setHttpDestination() function, typically retrieved through the Application property Url or by using the property’s synonymous variable `ServiceUrl`.
`setHttpDestination (*responseUrl*)`	Specifies the URL to which to post the SAML response in the response’s HTTP POST binding (the value in the “action=” argument). Typically a URL provided by retrieving the Application property Url or by using the property’s synonymous variable ServiceUrl. You can repeat this assertion-set function at the end of the script using a string to specify an absolute URI if you want to post the SAML response to a specific address, such as a proxy provided by a cloud access security broker (CASB).

global Function	Description
`setDigestMethodAlgorithm (*'algorithm'*)`	`setDigestMethodAlgorithm`specifies the digest method algorithm to use in the SAML response. Possible values are: sha1 sha256 sha384 sha512 The default value is the same as the `SignatureMethod` algorithm for the signing certificate selected for the app. For example, `setDigestMethodAlgorithm ('sha256')`.
`setAttribute(*elementName, elementValue*)`	This function is needed if the service provider requires a specific value, such as email, to be passed within the SAML assertion. Takes two arguments. The first is a string that specifies the name of a SAML response attribute to set, the second specifies the attribute value. For example, `setAttribute("Email", LoginUser.Get("mail"));` specifies the SAML attribute named "Email" to be set to the current user's email address. **Note**: Because Javascript treats the \ (backslash) character as an escape character, if you want to use a \ in your *elementValue*, you must precede it with another \. For example, if you want to use an *elementValue* of string "DOMAIN\user" in a SAML response attribute named "exampleAttr", you write: `setAttribute("exampleAttr", "DOMAIN\\\\user");`
`setAttributeArray (*elementName, elementArray*)`	Takes two arguments. The first is a string that specifies the name of a SAML response attribute to set, the second specifies an array as the attribute value. For example, `setAttributeArray('Groups', LoginUser.GroupNames);` specifies the SAML attribute named "Groups" to be set to an array of group names in which the current user is a direct member. **Note**: Because Javascript treats the \ (backslash) character as an escape character, if you want to use a \ in an *elementValue* in the *elementArray*, you must precede it with another \.

To enable autocomplete suggestions in the SAML Script Editor

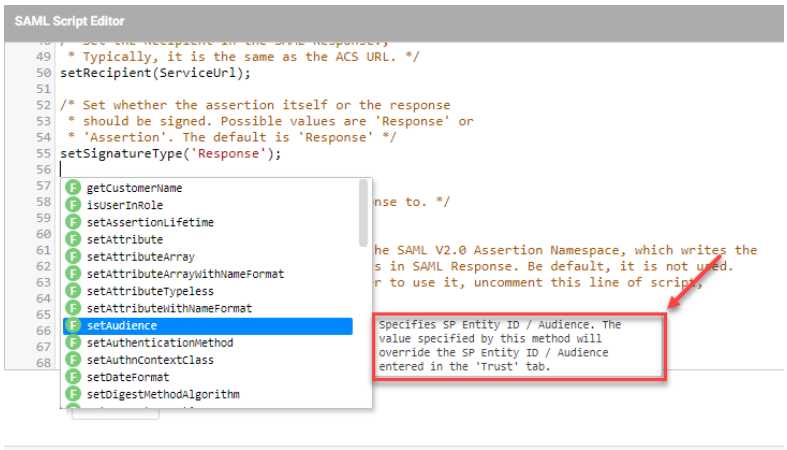
1. In the SAML Script Editor, press Ctrl+Spacebar.

   A menu appears showing available functions.



2. Use the arrow keys to select from available options, then press Enter to select the option.

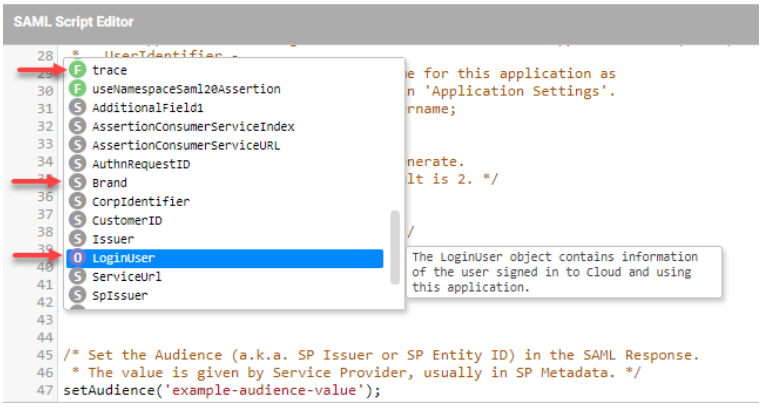
   Note the help text that appears with each selection.



   In addition, each available selection is coded based on type. For example:

   - F: Function
   - S: String

- O: Object

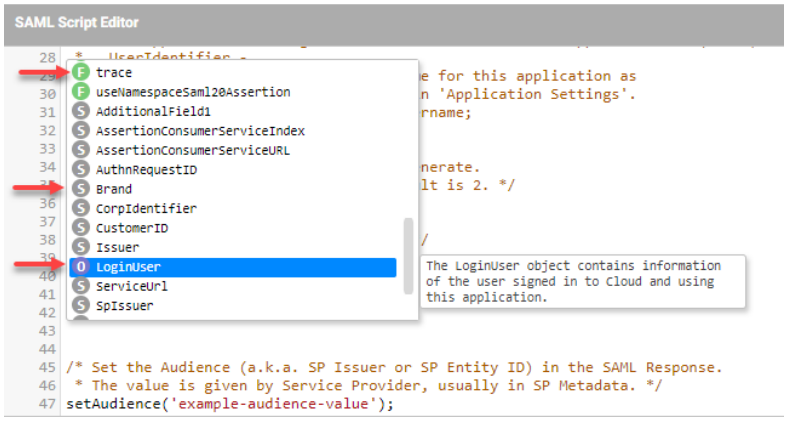


3. Continue editing the script, using Ctrl+Spacebar as necessary for suggestions.

   If you have already entered most of the function and only one possibility remains, Ctrl+Spacebar completes the string rather than showing available choices.

To enter a custom SAML script in the SAML Response page

1. Scroll down to the **Custom Logic** area and click in the SAML Script Editor where you want to edit the script.



2. Enter the SAML script in the text panel, replacing the existing script or using it as a template script.

   Remember that you can press Ctrl + Spacebar to enable the autocomplete feature. In addition, Script Help showing available methods, objects, and variables is available to the right of the Script Editor.

Incorrect JavaScript syntax in a line triggers a yellow symbol before the line number. Although the text panel offers this simple JavaScript support, if you're writing a script of any length you may want to use a specialized JavaScript editor and paste the results into the text panel.

Note: The template script present in the text panel by default will *not* work as a custom SAML script. You must modify or replace the script to meet the specific requirements of the web application.

3. (Optional) Click **Preview SAML Response**, then select a user to preview the results of the script for that user.

The Preview SAML Response window opens showing SSO Token details and the results of a trace of the script. The SSO token is generated by the Admin Portal for the user to log in to the web application.

4. Click **Save** .

Read "Custom SAML Applications" on page 961 for more information about using the generic SAML application template.

Example: Using Custom User Attributes

As part of configuring SAML applications, you can use JavaScript to define if users can be authenticated by the service provider (SP) using the custom attribute. In the sample script below, we are defining that all users with access to this application can be authenticated by the service provider (SP) using the custom attribute `(IsFull_TimeEmployee)`. "FullTime" is the corresponding SP attribute.

```
var um = module("User");

var u = um.GetUserData(null);

var IsFull_TimeEmployee = u.IsFull_TimeEmployee;

setAttribute("FullTime", IsFull_TimeEmployee);

The sample script below is specific to B2B SAML applications:

var fc =LoginUser.Get ("IsFull_TimeEmployee");

setAttribute("FullTime", IsFull_TimeEmployee);
```

Scripting Environment Reference

The Privileged Access Service creates a set of JavaScript objects, global variables, and global methods for each SAML user session. These objects provide information that a user map script or a custom SAML script can read

and act on. Some of the objects also accept values that specify elements with the SAML assertion that the Privileged Access Service presents to a web application.

This section describes the SAML user-session JavaScript environment in which the user map script and the custom SAML script execute. The section describes each available object and its public properties and methods. It also describes available global variables and global methods.

Application Object

The Privileged Access Service creates a single Application object for each SAML user session. The object is an instance of the `ReadOnlyDataEntity` class, and is a read-only object.

The Application object's properties describe the SAML web application as it's defined in the application profile. Create a SAML web application profile in the Admin Portal using the customSAML application template (described in "Custom SAML Applications" on page 961.

A script accesses the object's properties using the object's single public function.

Function Name	Description
`Application.Get (*property*)`	This function returns an Application object property. It takes as its argument a string that specifies the property to return. An example: `Application.Get("Name")` returns the name of the application as entered in the Application Settings tab.

The `Application.Get()` function may take the following property names as an argument. Each argument returns a different application property. The property names are case-sensitive.

Property Name	Description
`\_PartitionKey`	The customer ID used to establish the user session. An example: BZ284.
`\_RowKey`	The UUID (universally unique identifier) of the application.
`Description`	The text description of the web application entered in the description field of the Application Settings tab.
`Icon`	The graphic file used as the icon for this application as set in the Application Settings tab.
`Issuer`	The entity ID specified in the Issuer field of the Application Settings tab. Synonymous with the global variable Issuer.
`Name`	The name of the application as entered in the Application Settings tab.
`SamlScript`	The custom SAML script set in the Advanced tab.
`TemplateName`	The type of generic application template used to define this web application's profile. Possible return values: Generic SAML Generic User-Password

Property Name	Description
`Url`	The contact URL specified in the URL field in the Application Settings tab. Synonymous with the global variable ServiceUrl.
`UserName` Strategy	The technique specified in the Application Settings tab to determine the user name (user identity) for a user session. Possible return values: **ADAttribute**: the Privileged Access Service sets the user name to the specified AD attribute of the current user. The Privileged Access Service queries the connector for the AD attribute. The Privileged Access Service caches the user name so that it doesn't have to query the connector for this user's future sessions. **Fixed**: the Privileged Access Service sets the user name to the value entered in the Application Settings tab. **UseScript**: the Privileged Access Service executes the user map script to determine the user name.
`WebAppType`	The authentication function used by the web application. Possible return values: `SAML` `UsernamePassword`

Global Variables

The Privileged Access Service creates a set of global variables for each SAML user session. These variables are synonyms for common attributes of the `LoginUser` and `Application` objects, and are a convenience: you can use a global variable instead of specifying a LoginUser attribute or using `Application.Get()` to read an `Application` attribute.

global Variable	Description
`ApplicationUrl`	A variable that contains the string value specified in the Assertion Consumer Service URL field in the Application Settings tab. Synonymous with the Application attribute "Url."
`AssertionConsumerServiceIndex`	A variable in the SAML request that contains the Assertion Consumer Service index value used to identify the Assertion Consumer Service URL. This variable is mutually exclusive with `AssertionConsumerServiceURL`.
`AssertionConsumerServiceURL`	A variable that contains the specific Assertion Consumer Service URL that specifies the URL to which the Privileged Access Service sends the SAML response. This variable is mutually exclusive with AssertionConsumerServiceIndex.
`Issuer`	A variable that contains the entity ID specified in the Issuer field of the Application Settings tab. Synonymous with the Application attribute "Issuer."
`ServiceUrl`	A variable that contains the string value specified in the Assertion Consumer Service URL field in the Application Settings tab. Synonymous with the Application attribute "Url."

LoginUser Object

The Privileged Access Service creates a single `LoginUser` object for each SAML user session. The object is an instance of the LoginUser class, and is a read/write object.

The function `LoginUser.Get()` retrieves any one of the current user's attributes. It takes as its argument a string that specifies the key of the attribute to retrieve. `LoginUser.Get("mail")`, for example, returns the user's email address as stored in Active Directory.

When `LoginUser.Get()` executes, the Privileged Access Service contacts the source directory through the connector for the user's organization and retrieves the attribute. If, for example, an Active Directory user has logged into the Admin Portal as a member of the Acme organization, executing `LoginUser.Get()` during one of that user's log-on sessions contacts the Acme Active Directory service through the connector set up in Acme's internal network. If a user has logged in, executing `LoginUser.Get()` queries the Cloud Directory Service (CDS).

Note: Not all attributes are common between directory services. If you have uses managed by different directory services (for example, AD and LDAP), use the `LoginUser.ServiceType` or `Login.User.ServiceName` properties to determine the user's source directory and then get the appropriate attribute key. Refer to "LoginUser Object" above for more information.

Example

```
if(LoginUser.ServiceType == 'LDAPProxy'){

UserIdentifier = LoginUser.Get('uid');

} else {

UserIdentifier = LoginUser.Username;

}
```

Explanation

The preceding example checks to see if the user is managed by LDAP. If the user's service type is LDAPProxy, the script gets the current user's UID attribute, otherwise it uses the `LoginUser.Username` property.

The `LoginUser` object has the following methods:

Function name	Description
`LoginUser.Get(ADkey)`	This function returns any one of the current user's Active Directory attributes. It takes as its argument a string that specifies the key of the attribute to retrieve. An example: `LoginUser.Get("mail")` returns the user's email address as stored in the user's Active Directory account.

Function name	Description
`LoginUser.GetValues(ADkey)`	This function returns an array with all values of an Active Directory attribute with multiple values for the current user. It takes as its argument a string that specifies the key of the attribute to retrieve. For example, the line `setAttributeArray('proxies', LoginUser.GetValues('proxyAddresses'));` sets an attribute array named proxies that includes all values for the logged in user for the AD key `proxyAddresses`.
`LoginUser.GetGroupAttributeValues (ADkey)`	This function returns the values of the current user's groups specified AD attribute. It takes as its argument a string that specifies the key of the attribute to retrieve. An example: `LoginUser.GetGroupAttributeValues("sAMAccountName")` returns the user's groups `sAMAccountName` value as stored in the user's Active Directory account.

The `LoginUser` object's properties describe the user as he or she is presented to the web application. The following table describes those properties.

Property name	Description
`LoginUser.Username`	The user identity presented in the SAML assertion to the web application. The Privileged Access Service determines the user ID for this user session depending on the "Map to User Accounts" setting in the Application Settings tab. (These settings determine the user name, which is the user ID presented in the SAML assertion.)
`LoginUser.FirstName`	The first name of the user presented in the SAML assertion to the web application. Note the following special cases for parsing this attribute for users in directory services that do not have the FirstName attribute, such as Centrify Directory: `FirstName` attribute is parsed from the first string of `DisplayName`. If `DisplayName` is a single string, the same string is used for the `FirstName` and `LastName` attributes. If `DisplayName` is null, `FirstName` and `LastName` return as null. SAML apps that require non-empty values will fail to launch in this case.

Property name	Description
`LoginUser.LastName`	The last name of the user presented in the SAML assertion to the web application. Note the following special cases for parsing this attribute for users in directory services that do not have the `LastName` attribute, such as Centrify Directory: The `LastName` attribute is parsed from the last string of `DisplayName`. Any additional strings between the first string and the last string are ignored. If `DisplayName` is a single string, the same string is used for the `FirstName` and `LastName` attributes. If `DisplayName` is null, `FirstName` and `LastName` return as null. SAML apps that require non-empty values will fail to launch in this case.
`LoginUser.GroupNames`	An array of group names for groups in which the user is an effective member (according to the user's Active Directory account). A user is an effective member of a group if he is either a direct member of the group or is a direct member of a group that is in turn a member of the group. This property returns the same value as `LoginUser.EffectiveGroupNames`.
`LoginUser.GroupNames2`	
`LoginUser.RoleNames`	
`LoginUser.EffectiveGroupNames`	An array of group names for groups in which the user is an effective member (according to the user's Active Directory account). A user is an effective member of a group if he is either a direct member of the group or is a direct member of a group that is in turn a member of the group. This property returns the same value as `LoginUser.GroupNames`.
`LoginUser.GroupDNs`	An array of distinguished names of groups in which the user is an effective member. This property returns the same value as `LoginUser.EffectiveGroupDNs`.
`LoginUser.EffectiveGroupDNs`	An array of distinguished names of groups in which the user is an effective member. This property returns the same value as `LoginUser.GroupDNs`.
`LoginUser.ServiceType`	The type of directory service managing the user's user object. Possible values are: ADProxy, LDAPProxy, CDS (Cloud Directory Service), FDS (Federated Directory Service)
`LoginUser.ServiceName`	The name of the directory service managing the user's user object. These values are set by the network administrator. This property is useful in environments with more than one LDAP proxy.

Global Methods

The Privileged Access Service provides a set of global methods available in a SAML user session that specify elements within a SAML assertion.

Assertion-set Methods

Assertion-set methods set the attributes of the private SAML assertion object in a user session. The assertion object specifies how the Privileged Access Service constructs the SAML assertion for this SAML user session. Most of these methods take as an argument the value for a specific SAML assertion element. `setIssuer()`, for example, accepts an entity ID and uses it to specify the issuer URL in the SAML assertion.

Two of the assertion set methods, `setAttribute()` and `setAttributeArray()` specify a SAML response attribute by name and then specify a value for that attribute that is either a single argument or an array. Use these methods to add SAML assertion elements that can't be specified by any of the other assertion set methods.

The following table lists global assertion-set methods available in a user session.

global Method	Description
`setAttribute(elementName, elementValue)`	Sets a specified SAML assertion element to a value. Takes two arguments. The first is a string that specifies the name of a SAML assertion element to set, the second specifies that attribute's value. For example, `setAttribute("Email", LoginUser.Get("mail"));` specifies the SAML assertion element named "Email" to be set to the current user's email address. Note: Because Javascript treats the \ (backslash) character as an escape character, if you want to use a \ in your `elementValue`, you must precede it with another \. For example, if you want to use an elementValue of string "DOMAIN\user" in a SAML response attribute named "exampleAttr", you write: `setAttribute ("exampleAttr", "DOMAIN\\\\user");`
`setAttributeArray(elementName, elementArray)`	Sets a specified SAML assertion element to an array. Takes two arguments. The first is a string that specifies the name of a SAML assertion element to set, the second specifies an array as that attribute's value. For example, `setAttributeArray('Groups', LoginUser.GroupNames);` specifies the SAML assertion element named "Groups" to be set to an array of group names in which the current user is a direct member. Note: Because Javascript treats the \ (backslash) character as an escape character, if you want to use a \ in an elementValue in the elementArray, you must precede it with another \.
`setAudience(audience)`	Specifies the audience in an audience restriction in the SAML assertion. This argument typically takes a URL such as "https://login/myapp.com".

global Method	Description
`setAuthenticationMethod( authenticationUri)`	Specifies the type of authentication used to authenticate the user. This takes a URI as described in section 2.4.3 of the SAML 2.0 core specification. The same specification lists possible URI values in section 7.1. An example: `urn:oasis:names:tc:SAML:1.0:am:password` specifies that the user was authenticated via password.
`setHttpDestination (responseUrl)`	Specifies the URL to which to post the SAML response in the response's HTTP POST binding (the value in the "action=" argument). Typically a URL provided by retrieving the Application property Url or by using the property's synonymous variable `ServiceUrl`. You can repeat this assertion-set method at the end of the script using a string to specify an absolute URI if you want to post the SAML response to a specific address, such as a proxy provided by a cloud access security broker (CASB).
`setIssuer(issuer)`	Specifies the issuer in the SAML assertion. Typically a URL provided by retrieving the Application property Issuer or by using the property's synonymous variable `Issuer`.
`setNameFormat(format)`	Specifies the Format value (the value following "Format=") in the SAML assertion's `NameID` element. This element is only used in a SAML 2.0 assertion.
`setRecipient(recipient)`	Specifies the recipient in the SAML assertion's `SubjectConfirmationData` element. This typically takes a URL such as https://login/myapp.com".
`setDigestMethodAlgorithm ('algorithm')`	`setDigestMethodAlgorithm` specifies the digest method algorithm to use in the SAML response. Possible values are: sha1 sha256 sha384 sha512 The default value is the same as the SignatureMethod algorithm for the signing certificate selected for the app. For example, `setDigestMethodAlgorithm('sha256')`.
`setRelayState(relayState, overwrite)`	Takes two arguments. The first is a `relayState` parameter to send with the SAML response if specified by the service provider. This parameter is specified in section 3.6.3.1 of "Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0." The second is an optional boolean overwrite parameter that specifies whether the first `relayState` argument overwrites the SP's `RelayState`. For example, `setRelayState("/myapps-relay-state", true)`: always overwrites the SP's `RelayState` as `/myapps-relay-state.setRelayState ("/myapps-relay-state", false)`: does NOT overwrite the SP's `RelayState`. `setRelayState("/myapps-relay-state")` is the same as `relayState0`

global Method	Description
`setServiceUrl(targetUrl)`	Specifies the value for the `TARGET` form element (the resource requested for the user session) when posting the SAML response. This is typically a URL that is the same as that used for the `setHttpDestination()` method, typically retrieved through the Application property Url or by using the property's synonymous variable `ServiceUrl`.
`setSignatureType(signingPref)`	Specifies what should be signed using a certificate: the SAML assertion or the SAML response that contains the assertion. The two possible values are "Response" or "Assertion". The default is "Response" if this method isn't present in the script.
`setSubjectConfirmationMethod(methodUri)`	Specifies the SAML confirmation method identifier for the SAML assertion's binding. This takes a URI as described in section 4.1.2.1 of "Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0." An example: `urn:oasis:names:tc:SAML:1.0:cm:bearer` specifies the Bearer confirmation method.
`setSubjectName(username)`	Specifies the subject in the SAML assertion, which is the user identity (user name) presented to the SAML web application. It's typically provided by retrieving the `LoginUser.Username` property or by using the property's synonymous variable `UserIdentifier`.
`setVersion(samlVersion)`	Specifies the version of the SAML assertion. "1" specifies version 1.1, "2" specifies version 2.0. The default is 2 if this method isn't present in the script.

User-Password Application Scripting

You can use the custom user-password application template (described in "Adding User-password Applications" on page 975 to add a user-password web application to the Delinea App Catalog. This template creates a user-password application profile for a web application that defines how the Privileged Access Service logs an authenticated user on to the web application via an HTML reply form containing user and password information.

Each user-password application profile requires a custom user-password script. The script defines how the Privileged Access Service creates an HTML response to log on for each user's session with the web application. Each application profile may also provide an optional user map script that determines the user's application log-on name and password for use in the HTML response. Both scripts are written in JavaScript.

This guide provides these sections:

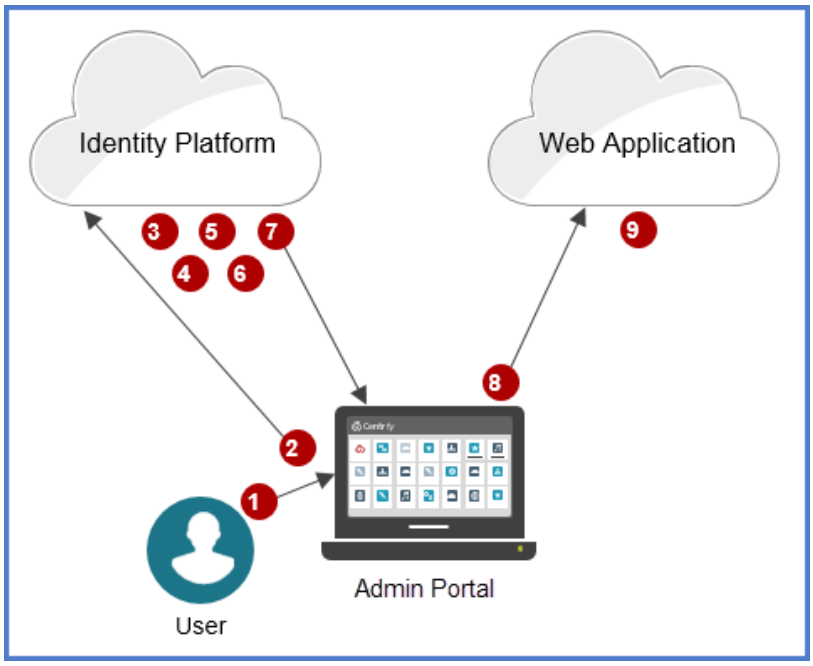
- "User-Password Authentication Overview" on the next page is an overview of the user-password authentication process for a user session with a web application. It shows how the Privileged Access Service works with a set of JavaScript objects during the process.

- "An Example Script" on page 1028 describes how you can write an optional user map script to specify an application user log-on name and password for a user session.
- "Writing a Custom User-Password Script" on page 1029 describes how to write the required custom user-password script to define an HTML response that authenticates the user for a user session.
- "Scripting Environment Reference" on page 1044 is a reference section for the objects, methods, and variables in the user map and user-password scripting environment.

To write a custom user-password script, you need to know how to write code in JavaScript. For the vast majority of user-password web applications, the script is simple and you won't need to do anything more than what's described in "Custom Apps Overview" on page 960. This guide is for the unusual application that might require more.

User-Password Authentication Overview

When the Privileged Access Service authenticates a user to a user-password web application, the Privileged Access Service creates an HTML response for the user session that satisfies the requirements of the web application and presents necessary information about the current user. The following figure shows user-password authentication steps. Step descriptions follow.



1. The user launches the web application in the Admin Portal.
2. The Admin Portal notifies the Privileged Access Service that the user wants a session with the web application.
3. The Privileged Access Service creates a set of JavaScript objects for this user-password user session:
   - An **Application object** that contains the properties of the web application as they're defined in the web application profile. Those properties are defined using the generic user-password application template and include the application name, the URL, the icon, and others that appear in the template in the Admin Portal. The Application object is a read-only object. A script reads its properties through the object's `Get()` method.

- A **LoginUser object** that contains information about the user identity used to log onto the service provider: the web application log-on user name (which is not necessarily the Admin Portal login user name) and so on. This is a read-write object that may be altered before it's used later in the custom user-password script to set the user name and password in the HTML response.
- A **response object** that defines the elements of the HTML response that the Privileged Access Service builds to send to the web application. The response object is a read/write object that the custom user-password script sets using the object's `AddFormField()` method.

4. The Privileged Access Service determines the web application log-on user name and password as specified in the generic user-password application template.The template specifies any one of these four methods:
   - The Privileged Access Service checks the user's Active Directory user record through the connector and retrieves the specified attribute as the application user name. It prompts the user for the password. The Privileged Access Service then assigns the user name to the LoginUser.Username property and the password to the `LoginUser.Password` property.

     The Privileged Access Service caches the returned user-name attribute so that it doesn't have to retrieve it again from Active Directory for later identical queries. The Privileged Access Service also stores the password locally so the user need not enter it again for future user sessions with this application.
   - The Privileged Access Service reads the shared single user name and password specified in the template and assigns them to `LoginUser.Username` and `LoginUser.Password`.
   - The Privileged Access Service prompts the user for the web application log-on user name and password and assigns them to `LoginUser.Username` and `LoginUser.Password`.

     The Privileged Access Service stores the user name and password locally so the user need not enter them again for future sessions with this application.
   - The Privileged Access Service executes the user map script set in the template, which creates a user name and assigns it to `LoginUser.Username`. The script may also create an optional password and assign it to `LoginUser.Password`.

     The Privileged Access Service prompts the user for a password in any case. If the script doesn't create its own password, the Privileged Access Service writes the entered password to LoginUser.Password and also stores the password locally so that the user need not enter it again for future sessions with this application. If the script creates its own password, the Privileged Access Service ignores the user's entered password.
5. The Privileged Access Service executes the custom user-password script to specify an HTML response for the user session.

   The script must include all the HTML response fields required by the web application and must provide appropriate values for those fields. Most applications require only a user field and a password field, but a few may require additional fields. The script uses `response.AddFormField()` to define the elements in the private assertion object.
6. The Privileged Access Service creates an HTML response based on the properties of the response object.
7. The Privileged Access Service sends the HTML response to the Admin Portal (or the browser running it). The HTML response includes a redirection that instructs the Admin Portal to send the response to the web application at the URL specified in the web application's profile.

The profile must contain a standard URL (set in the URL field of the generic user-password application template) and may also contain a mobile URL (set in the Mobile URL field). If the request for connection comes from a mobile device, the Privileged Access Service redirects the HTML response to the mobile URL if one exists, otherwise the Privileged Access Service redirects the response to the standard URL. If the request for connection is not from a mobile device, the Privileged Access Service redirects the response to the standard URL.

8. The Admin Portal sends the HTML response to the specified URL.
9. The web application reads the HTML response and then (if the response checks out) logs the user onto the web application.

User Map Script Elements

The user map script is an optional way to determine the user name and password to present to a web application. Use it if the other user-mapping options won't provide what's required. Your script can examine current application and user properties for this user session and can use that information and any other factors to create a user name and password. The user map script must, at some point, assign a user name to the `LoginUser.Username` property. It may also assign a password to the `LoginUser.Password` property, but it's not required. If the script doesn't create and assign a password, the Privileged Access Service gets the password by requesting it from the user. It then assigns the password to the `LoginUser.Password` property.

Retrieving Application Information

If the user map script requires information about the current web application, it can retrieve properties from the Application object created for this user session.

The method `Application.Get()` retrieves those properties. It takes as its argument a string that specifies the property whose value to retrieve. `Application("Name")`, for example, retrieves the name of the application.

"The Application Object" on page 1046 describes all of the Application object's properties that you may retrieve. These properties aren't typically used for determining a user name and password, although the application name may sometimes be useful.

Retrieving LoginUser Properties

If the user map script requires information about the current user settings, it can examine the properties of the `LoginUser` object created for this user session. "The LoginUser object" on page 1045 describes the `LoginUser` properties.

Several of these properties (`LoginUser.GroupNames`, for example) contain an array of group names of which the user is a member. These might be useful, depending on your requirements, for determining a user name. You might, for example, specify a single user name and password for anyone belonging to the admin group, and specify another single user name and password for anyone belonging to the sales group.

Retrieving the User's Active Directory Attributes

The `LoginUser` object offers a single method, `Get()`, that can retrieve any one of the current user's Active Directory attributes. It takes as its argument a string that specifies the key of the attribute to retrieve. `LoginUser.Get("mail")`, for example, returns the user's email address as stored in Active Directory.

When `LoginUser.Get()` executes, the Privileged Access Service contacts Active Directory through the connector for the user's organization and retrieves the attribute. If, for example, a user has logged into the Admin Portal as a member of the Acme organization, executing `LoginUser.Get()` during one of that user's log-on sessions contacts the Acme Active Directory service through the connector set up in Acme's internal network.

Specifying the User Logon Name

Once your script has created a web application log-on name as a string value, it must assign the name to the `LoginUser.Username` property. The script can assign the user name string directly to the property.

Specifying the Password

The script is not required to create a password, and often does not. If it does create a password as a string value, it must assign the password to the `LoginUser.Password` property so the custom user-password script can read the password later.

If the script doesn't assign a password value to `LoginUser.Password`, the Privileged Access Service determines the password value by asking the user for the password. The Privileged Access Service then assigns the user-provided password to `LoginUser.Password`. The Privileged Access Service also saves the password so that the user doesn't need to re-enter the password for later user sessions with the application.

An Example Script

This sample user map script creates a user name by adding the application name to the current user name in Active Directory. The script assigns the result to `LoginUser.Username`.

```
LoginUser.Username = LoginUser.Get("user") + "\#" + Application.Get("Name");
```

When the user whose AD account is "barney.blanton" wants to log into the web application named "Busfare," the script creates the user name "barney.blanton#Busfare". The script assigns the user name to LoginUser.Username, where the custom user-password script will find the user name later and use it for the HTML response.

Because the script does not create and assign a password to `LoginUser.Password`, the Privileged Access Service uses the password it receives when it prompts the user. The Privileged Access Service assigns the password to `LoginUser.Password` and then stores the password locally for later user sessions.

Writing a User Map Script

The user map script is JavaScript that you may create as an optional way to determine the user name and password used to log onto a web application.

Entering a User Map Script

To enter the user map script in the Application Settings tab of the generic user-password application template:

1. Under **Account Mapping**, select **Use Account Mapping Script** to open the user map script text panel.
2. Enter the script in the text panel.

   Incorrect JavaScript syntax in a line triggers a yellow symbol before the line number.
3. (Optional) Click **Test**.

The Test Results window opens showing Account Mapping Details and the results of a Trace of the script. The Account Mapping Details list displays the attributes of the mapped LoginUser.

4. Click **Save Changes**.

   Read "Custom User-password Applications" on page 955 for more information about using the generic user-password application template.

Writing a Custom User-Password Script

The custom user-password script specifies elements that must be present in the HTML response that starts the current user session with a web application. To write the script, you must know what HTML response fields the web application requires. The script must retrieve required information from the web application's profile and the user object, and must then specify the response fields and their values using the `response.AddFormField()` method. After the script executes, the Privileged Access Service follows the script's specifications to create an HTML response.

The custom user-password script is JavaScript. Each generic user-password application profile requires a custom user-password script.

Entering a Custom User-Password Script

To enter the custom user-password script in the Advanced tab of the generic user-password application template:

1. Click **Edit**.
2. Enter the advanced script in the text panel, replacing the existing script or using it as a template script.

   Incorrect JavaScript syntax in a line triggers a yellow symbol before the line number. Although the text panel offers this simple JavaScript support, if you're writing a script of any length you may want to use a specialized JavaScript editor and paste the results into the text panel.

   > The template script present in the text panel by default will in almost all cases *not* work as a custom user-password script for a web application. You must modify or replace the script to meet the specific response field requirements of the web application.

3. (Optional) Click **Test**.

   The Advanced Script Results window opens showing SSO Token details and the results of a trace of the script. The SSO token is generated by the Admin Portal for the user to log in to the web application.

4. Click **Save Changes**.

   Read "Adding User-password Applications" on page 975 for more information about using the generic user-password application template.

Determining HTML Response Requirements for the Web Application

Each user-password web application typically requires its own set of fields in an HTML response. The help text for the generic user-password application template describes how to use a browser to discover these fields in "Discovering the Login URL and Form Data Fields" on page 961. You may also use other HTML POST analysis tools to discover required fields.

Most user-password applications require only a user name field and a password field. Each application typically uses its own pair of field names for these fields, though, so it takes some customization to correctly set up the custom user-password script. The POST analysis may reveal extra required fields for a very few user-password applications. You may be able to guess what these fields must contain by their names and supply the proper values, but if not you'll need to contact the web application service provider's technical support or development team to ask for details.

Retrieving information

To retrieve information, the custom user-password script has access to the same JavaScript objects and global variables used in the user map script.

Retrieving application information

The read-only Application object created by the Privileged Access Service for a user session contains the properties defined in the application profile. Create a web application's profile using the generic user-password application template in the Admin Portal. You must set appropriate application properties in the application profile before the custom user-password script can retrieve application properties successfully.

The method Application.Get() retrieves application properties. It takes as its argument a string that specifies the property whose value to retrieve. Application.Get("Name"), for example, retrieves the name of the application.

"The Application Object" describes all the Application object's properties that you can retrieve. The following table shows two of the most useful application properties for user-password information. Note that these property names are case-sensitive. Note also that one of the properties has a synonymous global variable that you can use in place of using Application.Get().

Property name	Description
Name	The name of the application as entered in the Application Settings tab.
Url	The contact URL for the HTML response as specified in the URL field in the Application Settings tab. Synonymous with the global variable ServiceUrl.

Retrieving LoginUser properties

The properties of this user session's LoginUser object provide information about the user being authenticated for this user session. The following table describes the properties.

Property name	Description
LoginUser.Username	The username used to log the current user on to the web application. The Privileged Access Service determines the username for this user session depending on the "Map to user Accounts" setting in the Application Settings tab. This property is synonymous with the global variable UserIdentifier.

Property name	Description
LoginUser.Password	The password used to log the current user on to the web application. The Privileged Access Service determines the password for this user session depending on the “Map to user Accounts” setting in the Application Settings tab.
LoginUser.GroupNames	An array of group names for groups in which the user is an effective member (according to the user’s Active Directory account). A user is an effective member of a group if he is either a direct member of the group or is a direct member of a group that is in turn a member of the group. This property returns the same value as LoginUser.EffectiveGroupNames.
LoginUser.EffectiveGroupNames	An array of group names for groups in which the user is an effective member (according to the user’s Active Directory account). A user is an effective member of a group if he is either a direct member of the group or is a direct member of a group that is in turn a member of the group. This property returns the same value as LoginUser.GroupNames.
LoginUser.GroupDNs	An array of distinguished names of groups in which the user is an effective member. This property returns the same value as LoginUser.EffectiveGroupDNs.
LoginUser.EffectiveGroupDNs	An array of distinguished names of groups in which the user is an effective member. This property returns the same value as LoginUser.GroupDNs.

Retrieving LoginUser properties

The properties of this user session’s LoginUser object provide information about the user being authenticated for this user session. The following table describes the properties.

Property name	Description
LoginUser.Username	The username used to log the current user on to the web application. The Privileged Access Service determines the username for this user session depending on the “Map to user Accounts” setting in the Application Settings tab. This property is synonymous with the global variable UserIdentifier.
LoginUser.Password	The password used to log the current user on to the web application. The Privileged Access Service determines the password for this user session depending on the “Map to user Accounts” setting in the Application Settings tab.

Property name	Description
LoginUser.GroupNames	An array of group names for groups in which the user is an effective member (according to the user's Active Directory account). A user is an effective member of a group if he is either a direct member of the group or is a direct member of a group that is in turn a member of the group. This property returns the same value as LoginUser.EffectiveGroupNames.
LoginUser.EffectiveGroupNames	An array of group names for groups in which the user is an effective member (according to the user's Active Directory account). A user is an effective member of a group if he is either a direct member of the group or is a direct member of a group that is in turn a member of the group. This property returns the same value as LoginUser.GroupNames.
LoginUser.GroupDNs	An array of distinguished names of groups in which the user is an effective member. This property returns the same value as LoginUser.EffectiveGroupDNs.
LoginUser.EffectiveGroupDNs	An array of distinguished names of groups in which the user is an effective member. This property returns the same value as LoginUser.GroupDNs.

Retrieving the user's Active Directory attributes

The LoginUser object offers a single method, Get(), that can retrieve any one of the current user's Active Directory attributes. It takes as its argument a string that specifies the name of the attribute to retrieve. LoginUser.Get("mail"), for example, returns the user's email address as stored in Active Directory.

Defining HTML Response Fields

To define HTML response fields and set their values, use the response.AddFormField() method. It's a simple method that takes two arguments:

- *fieldname*, a string that defines the name of a field to add to the HTML response.
- *fieldvalue*, a string that defines the value presented in this HTML response field.

When executed, `response.AddFormField()` adds the defined field and its value to the response object. The Privileged Access Service reads the response object's field definitions when it's time to connect to the web application and creates an HTML response with those fields and their values.

It's best to supply the *fieldvalue* string by processing it through the global method encode(). This method ensures that the string is HTML-safe by properly encoding any special symbols such as @. The following example adds a field named "username-field" and sets its value to the current value of `LoginUser.Username`. The example uses `encode()` to ensure that whatever value is supplied is HTML safe:

```
response.AddFormField("username-field", encode(LoginUser.Username));
```

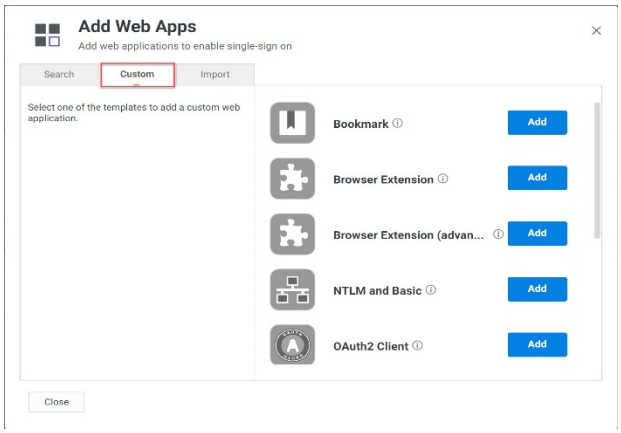
The custom user-password script should at least define a user-name field and a password field using whatever field names the web application requires. If the application requires additional fields, use `response.AddFormField()` to name those fields and set their values.

You'll find the response object and encode() method both described in "Scripting Environment Reference" on page 1044.

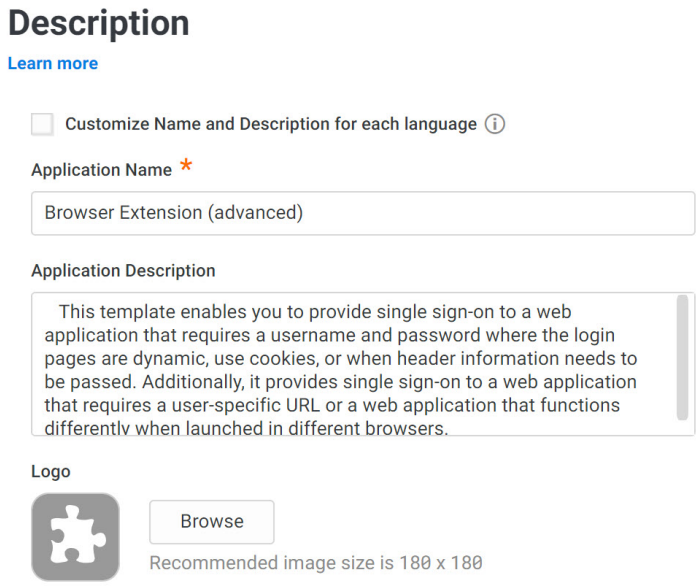
Adding and Configuring the Generic Browser Application

To add and configure a generic browser extension application:

1. In Admin Portal, click **Apps** > **Web Apps**. Click **Add Web Apps**. The Add Web Apps screen appears.
2. Click **Custom**. On the **Custom** tab, next to the **Browser Extension** application, click **Add**.

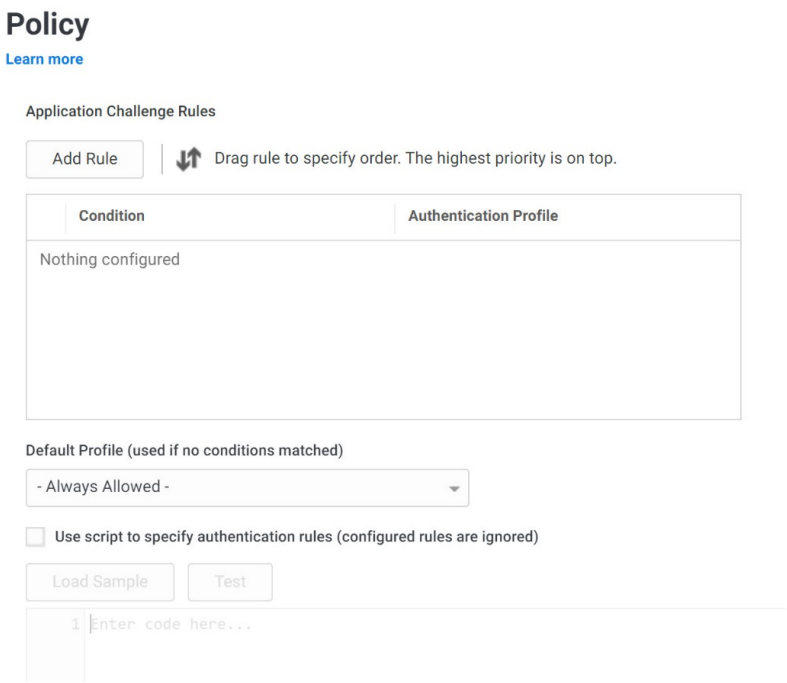


3. On the **Add Web App** screen, click **Yes** to add the application. The Admin Portal adds the application.
4. Click **Close** to exit the Application Catalog.
5. On the Web Apps page, choose the **Browser Extension** app you just added.
6. On the **Description** page, select if you'd like custom name and description for each language. Additionally, add the name, description, category, and logo for the application. For some applications, the name cannot be modified.



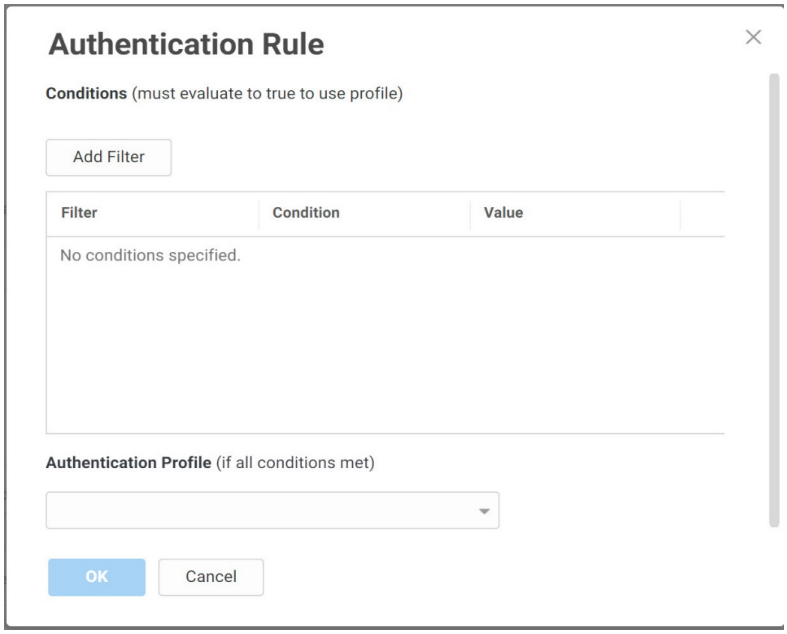
Note: Because this is a generic or custom application, it's recommended to give this application a unique name.

7. On the **Permissions** page, select the role(s), groups, and/or users that have access to the application.
8. (Optional) On the **Policy** page, specify additional authentication controls for this application. Here, you can add rules.



To add a rule:

1. Click **Add Rule**. The Authentication Rule window displays.



2. Click **Add Filter** on the Authentication Rule window.
   a. Define the filter and condition using the drop-down boxes. For example, you can create a rule that requires a specific authentication method when users access the Privileged Access Service from an IP address that is outside of your corporate IP range. Supported filters are:

Filter	Description
IP Address	The authentication factor is the computer's IP address when the user logs in. This option requires that you have configured the IP address range in Settings, Network, Corporate IP Range.
Identity Cookie	The authentication factor is the cookie that is embedded in the current browser by the Delinea PAS after the user has successfully logged in.
Day of Week	The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.
Date	The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.
Date Range	The authentication factor is a specific date range.
Time Range	The authentication factor is a specific time range in hours and minutes.

Filter	Description
Device OS	The authentication factor is the device operating system.
Browser	The authentication factor is the browser used for opening the Delinea PAS.
Country	The authentication factor is the country based on the IP address of the user computer.
Risk Level	The authentication factor is the risk level of the user logging on to user portal. For example, a user attempting to log in to Delinea PAS from an unfamiliar location can be prompted to enter a password and text message (SMS) confirmation code because the external firewall condition correlates with a medium risk level. This Risk Level filter, requires additional licenses. If you do not see this filter, contact Delinea PAS support. The supported risk levels are: Non Detected -- No abnormal activities are detected. Low -- Some aspects of the requested identity activity are abnormal. Remediation action or simple warning notification can be raised depending on the policy setup. Medium -- Many aspects of the requested identity activity are abnormal. Remediation action or simple warning notification can be raised depending on the policy setup. High -- Strong indicators that the requested identity activity is anomaly and the user's identity has been compromised. Immediate remediation action, such as MFA, should be enforced. Unknown -- Not enough user behavior activities (frequency of system use by the user and length of time user has been in the system) have been collected.
Managed Devices	The authentication factor is the designation of the device as “managed” or not. A device is considered “managed” if it is managed by Delinea PAS, or if it has a trusted certificate authority (CA has been uploaded to tenant).
For the Day/Date/Time related conditions, you can choose between the user’s local time and Universal Time Coordinated (UTC) time.	

3. Click the **Add** button associated with the filter and condition.
4. Select the profile you want applied if all filters/conditions are met in the **Authentication Profile** drop-down. The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the **Add New Profile** option. See "Creating Authentication Profiles" on page 284.
5. Click **OK.**

6. (Optional) In the **Default Profile (used if no conditions matched)** drop-down, you can select a default profile to be applied if a user does not match any of the configured conditions.
   If you have no authentication rules configured and you select **Not Allowed** in the **Default Profile** dropdown, users will not be able to log in to the service.
7. Click **Save**.
   If you have more than one authentication rule, you can prioritize them on the **Policy** page. You can also include JavaScript code to identify specific circumstances when you want to block an application or you want to require additional authentication methods. For details, see "Data That You Can Use in a Policy Script" on page 996.

   Note: If you left the Apps section of Admin Portal to specify additional authentication control, you will need to return to the Apps section before continuing by clicking **Apps** at the top of the page in Admin Portal.
8. On the **Account Mapping** page, configure how the login information is mapped to the application's user accounts.

   The options are as follows:

   - **Directory Service Field**: Use this option if the user accounts are based on user attributes. For example, specify an Active Directory field such as *mail* or *userPrincipalName* or a similar field from Delinea Directory. For Web - User Password applications, selecting this option allows an additional option to let Active Directory users log in using Active Directory credentials.
   - **Use the login password supplied by the user (Active Directory users only)** option for every Web - User Password application that you want users to log in to using Active Directory credentials.
   - **All users share one name**: Use this option if you want to share access to an account but not share the user name and password. For example, some people share an application developer account.
   - **Prompt for user name**: Use this option if you want users to supply their own user name and password. The first time a user launches the application, they enter their login credentials for that application. The Delinea PAS stores the user name and password and the next time the user launches the application, the Delinea PAS logs the user in automatically.
   - **Account Mapping Script**: You can customize the user account mapping here by supplying a custom JavaScript script. For example, you could use the following line as a script:

   LoginUser.Username = LoginUser.Get('mail')+'.ad';
9. The above script instructs the Delinea PAS to set the login user name to the user's mail attribute value in Active Directory and add '.ad' to the end. So, if the user's mail attribute value is Adele.Darwin@acme.com then the Delinea PAS uses Adele.Darwin@acme.com.ad. For more information about writing a script to map user accounts, see the "User-Password Application Scripting" on page 1024.
10. On the **Advanced** tab, configure how to submit the login and other authentication information for the application.

Browser Extension Variable field	Description	Examples
Host Name Suffix	Not used for now – for future use. If you don't specify this field, the Delinea PAS populates this with the last part of the domain of the URL.	For example, if the URL is signin.acme.com and you leave the host name suffix blank, the Admin Portal populates the host name suffix with acme.com.
User Name	The CSS Selector that matches the user name element.	input#userid input [name="username']
Password	The CSS Selector that matches the password element.	input#pass input#id_password
Submit	The CSS Selector that matches the submit button that transmits the authentication information for processing.	input#sgnBt input[value="Log In"] input.button-green
Form	The CSS Selector to select the HTML form element. This variable is optional, because not all web pages use forms. If the login page does use a form, you do need to specify it here in order for SSO to work.	form#login_form form.niceform
Additional Login Field	This CSS selector is for the additional login field, such as company ID.	input:imp
Additional Login Field Value	For applications that require an additional login field, you must specify the value. Users cannot enter the value.	1234
Selector Timeout	This optional field is for advanced users only. Use this field to indicate the number of milliseconds to wait for the expected input selectors to load before timing out on failure. A zero or negative number means no timeout.	1, 2, 3,... = number of milliseconds 0 or negative number = no timeout
Order	This optional field is for advanced users only. Use this field to specify the order of login if it is not username, password, and submit.	

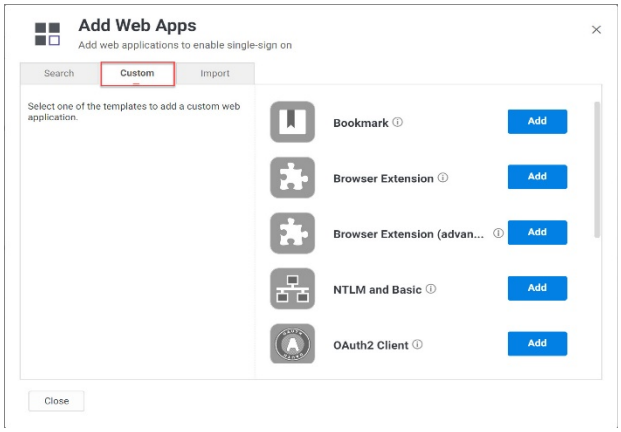
Tip: Make sure that your selectors are unique within the page that you're accessing. Otherwise, problems or data collisions can occur.

11. (Optional) Click **App Gateway** to allow users to securely access this application outside of your corporate network. For detailed configuration instructions, see "Configuring App Gateway" on page 980.
12. (Optional) On the **Changelog** page, you can see recent changes that have been made to the application settings, by date, user, and the type of change that was made.
13. (Optional) Click **Workflow** to set up a request and approval work flow for this application.
14. Click **Save**.

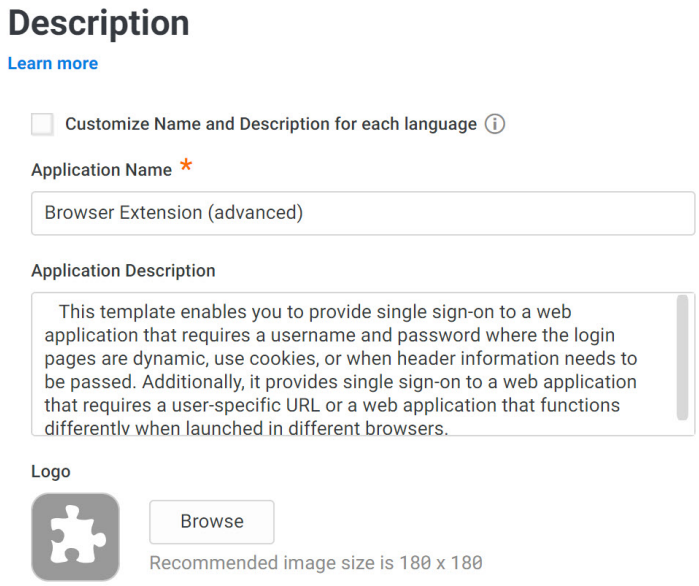
Adding and Configuring the Delinea Browser Extension (advanced) Application in the Admin Portal

To add and configure a Browser Extension (advanced) application:

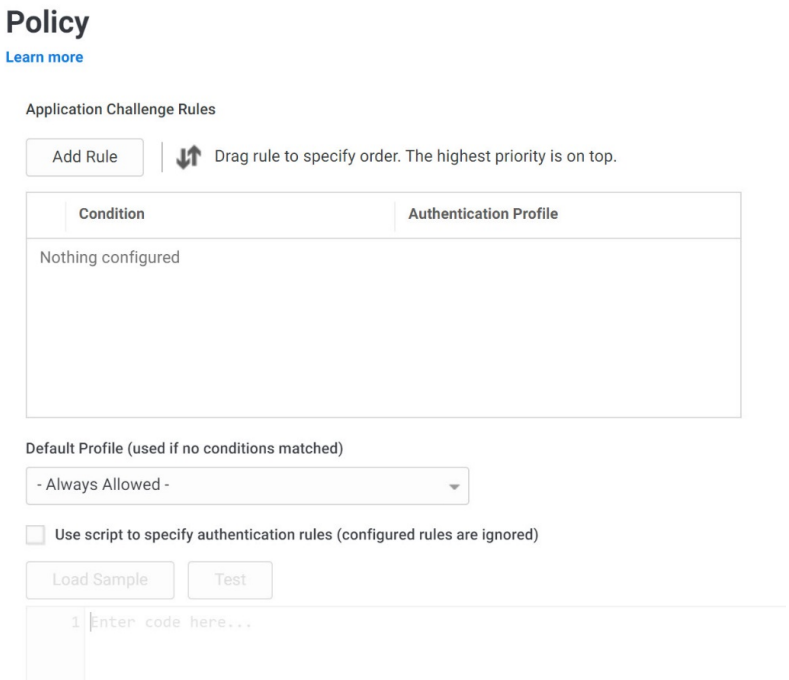
1. In the Admin Portal, click **Apps** > **Web Apps**. Click **Add Web Apps**. The Add Web Apps screen appears.
2. Click **Custom**. On the **Custom** tab, next to the **Browser Extension (advanced)** application, click **Add**.



3. On the **Add Web App** screen, click **Yes** to add the application. The Admin Portal adds the application.
4. Click **Close** to exit the Application Catalog.
5. On the Web Apps page, choose the **Browser Extension (advanced)** app you just added.
6. On the **Description** page, select if you'd like custom name and description for each language. Additionally, add the name, description, category, and logo for the application. For some applications, the name cannot be modified.

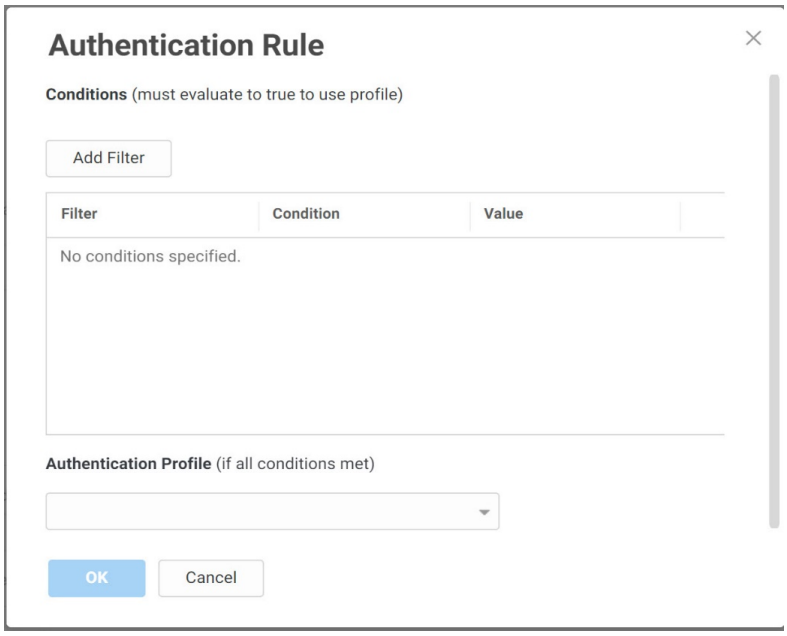


7. Because this is a generic or custom application, it's recommended to give this application a unique name.
8. On the **Permissions** page, select the role(s), groups, and/or users that have access to the application.
9. (Optional) On the **Policy** page, specify additional authentication controls for this application. Here, you can add rules.



To add a rule:

1. Click **Add Rule**. The Authentication Rule window displays.



2. Click **Add Filter** on the Authentication Rule window.
   a. Define the filter and condition using the drop-down boxes. For example, you can create a rule that requires a specific authentication method when users access Privileged Access Service from an IP address that is outside of your corporate IP range. Supported filters are:

Filter	Description
IP Address	The authentication factor is the computer's IP address when the user logs in. This option requires that you have configured the IP address range in Settings, Network, Corporate IP Range.
Identity Cookie	The authentication factor is the cookie that is embedded in the current browser by the Delinea PAS after the user has successfully logged in.
Day of Week	The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.
Date	The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.
Date Range	The authentication factor is a specific date range.
Time Range	The authentication factor is a specific time range in hours and minutes.

Filter	Description
Device OS	The authentication factor is the device operating system.
Browser	The authentication factor is the browser used for opening the Delinea PAS.
Country	The authentication factor is the country based on the IP address of the user computer.
Risk Level	The authentication factor is the risk level of the user logging on to user portal. For example, a user attempting to log in to Delinea PAS from an unfamiliar location can be prompted to enter a password and text message (SMS) confirmation code because the external firewall condition correlates with a medium risk level. This Risk Level filter, requires additional licenses. If you do not see this filter, contact Delinea PAS support. The supported risk levels are: Non Detected -- No abnormal activities are detected. Low -- Some aspects of the requested identity activity are abnormal. Remediation action or simple warning notification can be raised depending on the policy setup. Medium -- Many aspects of the requested identity activity are abnormal. Remediation action or simple warning notification can be raised depending on the policy setup. High -- Strong indicators that the requested identity activity is anomaly and the user's identity has been compromised. Immediate remediation action, such as MFA, should be enforced. Unknown -- Not enough user behavior activities (frequency of system use by the user and length of time user has been in the system) have been collected.
Managed Devices	The authentication factor is the designation of the device as “managed” or not. A device is considered “managed” if it is managed by Delinea PAS, or if it has a trusted certificate authority (CA has been uploaded to tenant).
For the Day/Date/Time related conditions, you can choose between the user’s local time and Universal Time Coordinated (UTC) time.	

3. Click the **Add** button associated with the filter and condition.
4. Select the profile you want applied if all filters/conditions are met in the **Authentication Profile** drop-down. The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the **Add New Profile** option. See "Creating Authentication Profiles" on page 284.
5. Click **OK.**

6. (Optional) In the **Default Profile** (used if no conditions matched) drop-down, you can select a default profile to be applied if a user does not match any of the configured conditions.
   If you have no authentication rules configured and you select **Not Allowed** in the **Default Profile** dropdown, users will not be able to log in to the service.
7. Click **Save**.
   If you have more than one authentication rule, you can prioritize them on the **Policy** page. You can also include JavaScript code to identify specific circumstances when you want to block an application or you want to require additional authentication methods. For details, see "Data That You Can Use in a Policy Script" on page 996.
8. If you left the Apps section of Admin Portal to specify additional authentication control, you will need to return to the Apps section before continuing by clicking **Apps** at the top of the page in Admin Portal.
9. On the **Account Mapping** page, configure how the login information is mapped to the application's user accounts.

   The options are as follows:

   Use the following Directory Service field to supply the user name: Use this option if the user accounts are based on user attributes. For example, specify an Active Directory field such as *mail* or *userPrincipalName* or a similar field from Delinea Directory.

   For Web - User Password applications, selecting this option allows an additional option to let Active Directory users log in using Active Directory credentials. Select the **Use the login password supplied by the user (Active Directory users only)** option for every Web - User Password application that you want users to log in to using Active Directory credentials.

   Everybody shares a single user name: Use this option if you want to share access to an account but not share the user name and password. For example, some people share an application developer account.

   Prompt the user for their user name: Use this option if you want users to supply their own user name and password. The first time a user launches the application, they enter their login credentials for that application. The Delinea PAS stores the user name and password and the next time the user launches the application, the Delinea PAS logs the user in automatically.

   Use Account Mapping Script: You can customize the user account mapping here by supplying a custom JavaScript script. For example, you could use the following line as a script:

   ```
   LoginUser.Username = LoginUser.Get('mail')+'.ad';
   ```

   The above script instructs the Delinea PAS to set the login user name to the user's mail attribute value in Active Directory and add '.ad' to the end. So, if the user's mail attribute value is Adele.Darwin@acme.com then the Delinea PAS uses Adele.Darwin@acme.com.ad. For more information about writing a script to map user accounts, see the "User-Password Application Scripting" on page 1024.

   On the **Advanced** tab, click **Edit** to enter or modify the JavaScript that specifies the login data that the Delinea PAS sends to the web application login URL when a user requests the application. This advanced script must be present and configured to match the service provider's required form fields.

   The default example script shows how to specify form fields. The example script does *not* work as is, and you must modify the script to match the requirements of each application. For the vast majority of web applications, you need to replace only the following:

- "<url>" (line 1) = Replace with the application URL.
- "<username selector>" (line 2) = Replace this with the application selector object for name.
- "<password selector>" (line 3) = Replace this with the application selector object for password.
- "<submit selector>" (line 4) = Replace this with the application selector object for submit.
- "<form selector>" (line 5) = Replace this with the application selector object for form.

The following is an example using username and password:

```
loginData.addField("username", "input\#username1", LoginUsername);

loginData.addField("password", "input\#password1", LoginPassword);
```

10. (Optional) Click **App Gateway** to allow users to securely access this application outside of your corporate network. For detailed configuration instructions, see "Configuring App Gateway" on page 980.
11. (Optional) On the **Changelog** page, you can see recent changes that have been made to the application settings, by date, user, and the type of change that was made.
12. (Optional) Click **Workflow** to set up a request and approval work flow for this application. See Configuring a request and approval workflow for more information.
13. Click **Save**.

Using the Custom User-Password Script Template

You can use the sample user-password script in the Advanced tab as a template for your own custom user-password script. The first two lines set values for the fields “username-field” and “password-field”, which are probably *not* the field names required by a specific user-password web application. Simply replacing those field names with the field names an application requires will satisfy most applications.

The third and forth lines add a third and fourth field to the response, which probably aren’t necessary. You can delete them if they aren’t. If an application requires additional fields, modify these lines with the required field names and values.

To see further examples of custom user-password scripts, select any already-defined user-password application profile in the Apps panel of the Admin Portal, then view its Advanced tab. The tab displays the custom script used to connect to that application.

Scripting Environment Reference

The Privileged Access Service creates a set of JavaScript objects, global variables, and global methods for each user-password user session. These objects provide information that a user map script or a custom user-password script can read and act on. Some of the objects also accept values that specify elements with the HTML response that the Privileged Access Service presents to a web application.

This section describes the user-session JavaScript environment in which the user map script and the custom user-password script execute. The section describes each available object and its public properties and methods. It also describes available global variables and global methods.

The LoginUser object

The Privileged Access Service creates a single `LoginUser` object for each user session for a user-password web application. The object is an instance of the `LoginUser` class, and is a read/write object.

The `LoginUser` object's properties describe the user as he or she is presented to the web application. The following table describes those properties.

Property name	Description
`LoginUser.Username`	The username used to log the current user on to the web application. The Privileged Access Service determines the username for this user session depending on the "Map to User Accounts" setting in the Application Settings tab.
`LoginUser.FirstName`	The first name of the user presented in the SAML assertion to the web application. Note the following special cases for parsing this attribute for users in directory services that do not have the `FirstName` attribute, such as Centrify Directory: `FirstName` attribute is parsed from the first string of `DisplayName` if `DisplayName` is a single string, the same string is used for the `FirstName` and `LastName` attributes if `DisplayName` is null, `FirstName` and `LastName` return as null. SAML apps that require non-empty values will fail to launch in this case.
`LoginUser.LastName`	The last name of the user presented in the SAML assertion to the web application. Note the following special cases for parsing this attribute for users in directory services that do not have the `LastName` attribute, such as Centrify Directory: The `LastName` attribute is parsed from the last string of `DisplayName`. Any additional strings between the first string and the last string are ignored. If `DisplayName` is a single string, the same string is used for the `FirstName` and `LastName` attributes. If `DisplayName` is null, `FirstName` and `LastName` return as null. SAML apps that require non-empty values will fail to launch in this case.
`LoginUser.Password`	The password used to log the current user on to the web application. The Privileged Access Service determines the password for this user session depending on the "Map to User Accounts" setting in the Application Settings tab. This property is synonymous with the global variable `LoginPassword`.
`LoginUser.GroupNames`	An array of group names for groups in which the user is an effective member (according to the user's Active Directory account). A user is an effective member of a group if he is either a direct member of the group or is a direct member of a group that is in turn a member of the group. This property returns the same value as `LoginUser.EffectiveGroupNames`.

Property name	Description
`LoginUser.EffectiveGroupNames`	An array of group names for groups in which the user is an effective member (according to the user's Active Directory account). A user is an effective member of a group if he is either a direct member of the group or is a direct member of a group that is in turn a member of the group. This property returns the same value as `LoginUser.GroupNames`.
`LoginUser.GroupDNs`	An array of distinguished names of groups in which the user is an effective member. This property returns the same value as `LoginUser.EffectiveGroupDNs`.
`LoginUser.EffectiveGroupDNs`	An array of distinguished names of groups in which the user is an effective member. This property returns the same value as `LoginUser.GroupDNs`.

The `LoginUser` object has a single method that a script may call:

Method name	Description
`LoginUser.Get (*ADkey*)`	This method returns any one of the current user's Active Directory attributes. It takes as its argument a string that specifies the key of the attribute to retrieve. An example: `LoginUser.Get("mail")` returns the user's email address as stored in the user's Active Directory account.

The Application Object

The Privileged Access Service creates a single Application object for each user session for a user-password web application. The object is an instance of the `ReadOnlyDataEntity` class, and is a read-only object.

The Application object's properties describe the web application as it's defined in the application profile. You create a web application's profile in the Admin Portal using the generic user-password application template (described in "Custom User-password Applications" on page 955.

The Application object does not have any publicly accessible properties. The script accesses the object's properties using the object's single public method, `Application.Get()`.

Method Name	Description
`Application.Get (*property*)`	This method returns an Application object property. It takes as its argument a string that specifies the property to return. An example: `Application.Get("Name")` returns the name of the application as entered in the Application Settings tab.

The following section describes the property arguments this method can take.

Application Properties

The `Application.Get()` method may take the following property names as an argument. Each argument returns a different application property. The property names are case-sensitive.

Property Name	Description
`\_PartitionKey`	The customer ID used to establish the user session. An example: BZ284.
`\_RowKey`	The UUID (universally unique identifier) of the application.
`Description`	The text description of the web application entered in the description field of the Application Settings tab.
`Icon`	The graphic file used as the icon for this application as set in the Application Settings tab.
`Name`	The name of the application as entered in the Application Settings tab.
`TemplateName`	The type of generic application template used to define this web application's profile. Possible return values: Generic SAML Generic User-Password
`Url`	The contact URL specified in the URL field in the Application Settings tab. Synonymous with the global variable ServiceUrl.
`UserName` Strategy	The technique specified in the Application Settings tab to determine the user name for a user session. Possible return values: **ADAttribute**: the Privileged Access Service sets the user name to the specified AD attribute of the current user. If this is a user-password web application, the Privileged Access Service asks the user to enter a password the first time the user asks for a connection to this web application. The Privileged Access Service stores the password for subsequent connections. **Fixed**: the Privileged Access Service sets the user name to the value entered in the Application Settings tab. If this is a user-password web application, this technique also sets the password to the value entered in the Application Settings tab. **SetByUser**: the Privileged Access Service asks the user to enter a user name the first time the user asks for a connection to this web application. If this is a user-password web application, the Privileged Access Service also asks for a password. The Privileged Access Service stores the user name (and password if applicable) for subsequent connections. **UseScript**: the Privileged Access Service executes the user map script to determine the user name.
`UserPassScript`	The custom user-password script set in the Advanced tab.
`WebAppType`	The authentication method used by the web application. Possible return values: SAML UsernamePassword

The Response Object

The Privileged Access Service creates a single response object for each user session for a user-password web application. The object is an instance of the `WebSignInResponse` class and is a read-write object.

The response object defines the HTML response that the Privileged Access Service creates to send to the web application. The object does not have any publicly accessible properties. The script defines HTML response fields using the object's single public method, `response.AddFormField()`.

Method Name	Description
`response.AddFormField( *fieldname, fieldvalue*)`	This method defines an HTML response field to add to the HTML response for this user session. The method takes as its first argument a string that specifies the property to return. Its arguments are: *fieldname,* a string that defines the name of the HTML response field. *fieldvalue,* a string that defines the value presented in the HTML response field. It's best to supply this string processed through the global method encode(), which ensures that the string is HTML-safe by properly encoding any special symbols such as @.

An example of setting an HTML response field:

```
response.AddFormField("username", encode(LoginUser.Username));
```

This example adds an HTML response field named "username" and sets its value to the current user name specified in the `LoginUser` object. The `encode()` method ensures that there are no non-HTML-compliant characters in the string returned by the attribute `LoginUser.Username`.

Global Variables

The Privileged Access Service creates a set of global variable for each user session. These variables are synonyms for common attributes of the `LoginUser` and `Application` objects, and are a convenience: you can use a global variable instead of specifying a `LoginUser` attribute or using `Application.Get()` to read an `Application` attribute.

global Variable	Description
`ApplicationUrl`	A read-only variable that contains the contact URL specified in the URL field in the Application Settings tab. Synonymous with the Application attribute "Url".
`LoginPassword`	A read-write variable that contains the password used to log the current user on to the web application, used only for a user-password application. The Privileged Access Service determines the password for this user session depending on the "Map to User Accounts" setting in the Application Settings tab. Synonymous with the attribute `LoginUser.Password.`
`ServiceUrl`	A read-only variable that contains the contact URL specified in the URL field in the Application Settings tab. Synonymous with the Application attribute "Url".

Global Functions

The Privileged Access Service provides global functions available in a user session for a user-password application.

Function Name	Description
`encode (*stringvalue*)`	This function takes a string as its argument and returns an HTML-safe version of the string for transmission via HTML. It converts each non-HTML-safe character into a string that the receiver will interpret as the original character.
`Hash (*stringvalue*, *hashalgorithm*, “x2”)`	This function takes a string and hash algorithm as arguments and returns a hash in the specified algorithm. Supported algorithms are: SHA-1 SHA-256 MD5 For example: `var hashedValue = Hash("raw_string", "sha256", "x2");`

Reviewing the Job History

The Privileged Access Service creates jobs automatically based on either a daily schedule or an event, or you can manually initiate different types of jobs. You can use the Job History to learn more about jobs processed in the last 30 days.

- Who requested the job.
- When the job started and completed.
- When the email notification was sent.

> Jobs older than 30 days are deleted from the job history.

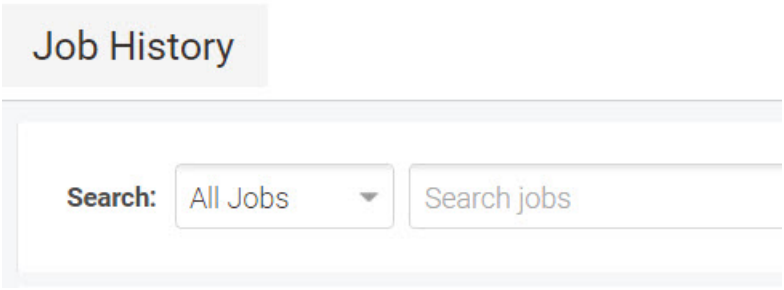
This section includes the following topics:

- "Searching for Jobs" below.
- "Downloading a Job Report" on the next page.
- "Viewing Job Details" on the next page.
- "Canceling Jobs" on the next page.
- "Deleting a Job" on page 1051.

Searching for Jobs

Use the available search functionality to find the job you want to learn more about. Search functionality includes the following:

- Searching by keywords.
- Filtering by job type or status (click the down arrow in the search field to view available job filters).



Downloading a Job Report

The Job Report tab of the Job History page shows a truncated version of the job report for convenience. You can download the entire report in a zip file for additional detail.

To download the job report:

1. Use the Search functionality to find the job that you want to download a report for, then click the job.

   A truncated version of the job report appears.
2. Click **Download Report**.

   A Save As dialog box appears.
3. Save the report.

   Reports are .txt documents compressed in a zip file.

Viewing Job Details

The Job Details tab provides details about a job that can help you troubleshoot

1. Use the Search functionality to find the job that you want to view additional details for, then click the job.
2. Click **Details** to see additional job details.

The Job Details tab appears, showing additional detail about the selected job.

Canceling Jobs

You can cancel Pending or Running jobs if you want to start a new job to capture new changes that occurred after the current job started. For example, if you have a long-running provisioning job and you want to capture changes to user objects that occurred after the job started, you can cancel the job and start over.

When a canceled job exits, any changes made by the job to that point remain intact. For example, user objects provisioned prior to cancellation remain provisioned. Start a new provisioning job to complete the provisioning.

To cancel one or more jobs:

Right-click a job and select **Cancel** or check the box next to each job that you want to cancel and then select **Cancel** from the Actions menu.

The job status changes to `CancellationRequested`, and then to `Canceled` once the job successfully exits.

If you can't successfully cancel the job, the status changes to `ProcessFailed`, and one of the following appears in the `SubStatus` column:

`NotFoundRunning` - Although the Job History indicated the job was running, it was not found. You can delete the job from the Job History.

`NotFoundCreated` - The pending job was never created, so there is no job to cancel. You can delete the job from the Job History.

Deleting a Job

You can delete completed jobs that are no longer relevant to you. You cannot delete jobs with a status of `Pending` or `Running`.

To delete a single job:

- Right-click a job and select **Delete**.

To delete multiple jobs:

1. Click the check box next to each job that you want to delete.
2. Click **Actions**, then select **Delete**.

Using the Workspace

The Workspace provides an overview of your own password checkout and session activity, including a list of the accounts for which you have a password checked out, your current sessions, and the servers and devices you have identified as favorites. In addition to providing an overview of rights that have been added to Privileged Access Service, when you log in to the Admin Portal with no administrative rights, you are granted access to **Workspace**. This allows you to provision accounts to users without granting them administrative rights.

You can view the following information in the Workspace:

- **My Expiring Checkouts** provides a quick reference for the number of passwords you have checked out that are due to be checked in within the next 15 minutes or have expired because they have not been checked in by their due date.
- **My Total Checkouts** summarizes the total number of passwords you have checked out.
- **My Total Sessions** summarizes the total number of sessions you have running on target systems.
- **Recent Systems** lists the systems you have accessed most recently.
- **My Password Checkouts** lists the accounts for which you have password currently checked out, when the password is due to be checked in, and the number of minutes remaining before the password expires. The number of minutes a password is allowed to be checked out can be configured on a server or device basis using the **Checkout lifetime** policy.
- **My System Accounts** lists the accounts the user has Workspace Login permission. It lists the system, account, and the credential type. For more information on **My System Accounts**, see "Using my System Accounts" on the next page
- **My Active Sessions** lists your currently active sessions, including the DNS name or IP address where the session is running, the user account under which the session is running, and the date and time the session

started.

- **My Favorites** lists the systems and local, domain, and database accounts you have identified as favorites in the system list on the Systems tab or the account list on the Accounts tab.

Managing an Active Session

If you are logged on with an account that has the Manage Session permission, you can watch or terminate active sessions from the Privileged Access Service dashboard. If your account does not have the Manage Session permission, the options to Watch or Terminate a session are not displayed the Actions menu.

To watch or terminate an active session:

1. Click **Resources > Dashboards**.
2. Select an active session from the Active Sessions list to display the Actions menu.
3. Select Watch to view the activity taking place in the selected session or Terminate to end the selected session.

Using my System Accounts

When an administrator provides **Workspace Login** on the account and view permission on the system for a user, the user will see that account on the **My System Account** in the Workspace.

Checking in a Password from the Workspace

After you check out a password, you have a limited period of time in which the password you checked out is valid for activity on a target system. When you end the session on the remote server, you should check in the password so that a new secure password can be generated for the account you used. From the Workspace tab, you can see a summary of your currently checked out account passwords at a glance.

To check in a password from the Workspace:

1. Click **Workspace** in the Admin Portal.
2. Select the system and account combination from the My Password Checkouts list.
3. Click the Actions menu, then select **Checkin**.

Working with Favorites from the Workspace

If you have identified any servers or network devices as favorites in the server list, you can use the Workspace to manage accounts, log in remotely, or delete the server or network device.

To work with a server or network device from the Workspace:

1. Click **Workspace** in the Admin Portal.
2. Select a system or account from the list of Favorites.
3. Click the **Actions** menu, then select the appropriate action.

   The actions available on the Actions menu depend on what you have selected. For example, if you select a favorite system, you might see the following actions:

- **Select/Request Account** to search for and select the account to use to log on the selected server or network device.
- **Enter Account** to log on remotely to the selected server or network device using a user name and password of your choice.
- **Add to Set** to add the selected server or network device to a new or existing set.
- **Delete** to delete the selected server or network device if all accounts for the server or network device have been deleted.

After you select an action, the next steps depend on the specific action you selected.

Managing your Sessions from the Workspace

If you have active sessions on one or more target systems, you can watch or terminate those sessions from the Workspace. Your account does not need to be granted the Manage Session permission to watch or terminate your own session.

To watch or terminate an active session:

1. Click **Workspace** in the **Admin Portal.**
2. Select an active session from the My Active Sessions list to display the Actions menu.
3. Select Watch to view the activity taking place in the selected session or Terminate to end the selected session.

Accessing Reports and Dashboards

You can access reports to find out specific information about your data and then share that information with other Privileged Access Service administrators. A report is a SQL query against your database tables and the results that the query generates. You can create reports and use the built-in reports as a way to find out specific information about your data. You can use the dashboard pages to view summaries and graphical representations of your Privileged Access Service usage.

- "Managing Reports" below
- "Viewing Dashboards" on page 1069

Managing Reports

You can create reports to find out specific information about your data and then share that information with other Privileged Access Service administrators. A report is a SQL query against your database tables and the results that the query generates. You can create reports as a way to find out specific information about your data: applications, devices, users, roles, connectors, and so forth.

You can use the default, built-in reports, or you can search for specific kinds of data by building your own report queries. You can also share reports with your other Privileged Access Service administrators.

What's in the Report Library

Use the Reports page to view, create, and share your reports. When you click Reports, the page opens to the My Reports folder. This folder lists all of the reports you have created. If you have not created any reports of your own, you might want to start by browsing through the predefined reports provided in the Builtin Reports folder and its subfolders. For example, if you expand the Builtin Reports folder and select the Mobile subfolder, you would see a list of the prebuilt reports for mobile devices.

Admin Portal provides the following folders to store reports:

- **Builtin Reports**: Admin Portal provides some prebuilt reports in this folder. You can specify parameters, such as date ranges, for some reports. These built-in reports demonstrate the kinds of data you can gather and display in your reports. You can copy these reports into your My Reports folder or the Shared Reports folder. After you copy a report to another location you can then modify the report.
- **My Reports**: When you create a new report or modify a report, Admin Portal saves it here. You can also copy built-in or shared reports to this folder so that you have all the reports that you use in one place. Only you can see the reports in your My Reports folder. You can also export, move, or delete reports in this folder.
- **Shared Reports**: To share reports with other administrators, you move or copy the reports here.

Exporting a report creates a file on your computer; you can specify either CSV or Microsoft Excel format. Copying a report duplicates the report into another reports folder.

Access to Shared Reports and Report Data

When you view a report, you can only read the data that you have permission to access. If you don't have read permission to a particular kind of data, such as applications, devices, or users, then the report doesn't display that information for you. (Permissions are granted to roles by the sysadmin—see "Admin Portal Administrative Rights" on page 277 for the details.

Note: The report doesn't indicate any limitations to that user's permissions. This means that people with different permissions can view the same report but see different results.

You can share any report in the Shared Reports folder. Sharing a report involves assigning it to specific roles and also to the folder(s) that contain the report.

When you assign a report or a report folder to a role, you also specify the level of access that the role has—read access, read and write access, or owner access. If you specify a role as an owner of a report or a report folder, then that role can modify, rename, share, or delete the report.

There are three kinds of access permission for reports:

- The level of access to the report definition
- Access to the data that is read by the report
- Access to the folder that contains the report

The report access level determines whether you can read, copy, modify, or share the report definition.

You can create reports in the Shared Reports folder, or you can copy reports from either the My Reports or Builtin Reports folders into the Shared Reports folder.

When you modify a report in the Shared Reports folder, you can also assign the report to roles. When you assign the report to a role, you also specify what the administrators in that role can do with the report by specifying either the Read, Read and Write, or Owner access. You also specify similar levels of access for the report folders.

- **Read**: Administrators can view and copy the report, but they cannot modify it, move it, or share it.
- **Read and Write**: Administrators can view, copy, move, and modify the report.
- **Owner**: Administrators can view, copy, move, and modify the report. Administrators can also grant other administrators access to the report.

At the minimum, you need to assign administrators to a role with at least the Read Only System Administration permission to enable them to view built-in and their own reports.

To share reports, you need to assign administrators to a role with Report Management permission.

However, you also need to grant administrators access to the types of data that you want them to view in the report. Administrators do not see report data for which they do not have permission to view.

Administrators can always view report data related to their own mobile devices.

For example, if an administrator has the Application Management permission but not the Device Management permission, when that administrator opens a report that generates both application and device results, the administrator sees only the application data.

How to Create a New Report

You can create new reports using SQL and parameters. Using parameters in your SQL query allows you to run the same report against different values instead of creating multiple reports.

To create a new report:

1. Log in to Admin Portal.
2. Click **Reports** > **New Report**.
3. Enter a name for your report.

   Names can contain letters, numbers, and underscores. Do not include special characters or white space.
4. Use the Data Dictionary column drop-downs to define what you want the report to display.

   The data dictionary has a list of all tables. After you select a column, tables not valid for a join are automatically disabled. If more than two tables are joined, and one table no longer has any filters and columns, then only tables that can be joined together will remain selected and in the SQL. For example, if A is joined to B is joined to C, and B is removed, and A and C cannot be joined, then only A will remain in the SQL.

   You can click the filter icon associated with each column to specify conditions for filtering on that column. Only the IN and NOT IN operations allows for multiple values.
5. (Optional) Use the script editor to manually build your report.

   See "Report Query Syntax" for help with syntax.

   Write SQL queries that use parameters for arguments rather than concrete values. This will allow you to run the same report against different values. For example, you can write the following SQL query:

   select username, lastlogin from user where username like @userParam

You now must define the “userParam” parameter to make use of the query.

6. Click **Parameters** to specify parameters.

   Parameters allow you to define a report with different values. Parameters you specify must be paired with your SQL query. In our example, the SQL query in the above step uses the “userParam” parameter, so you must define the same parameter here.

7. Click **Settings** to configure the report options:
   - Reports can be displayed on a map -- Enable this option to display the data on a map if the report is location related.
   - Validate reports on save (enabled by default) -- Enable this option to validate the SQL syntax when you save the report.

8. Click **Save**.

   Admin Portal saves your report to the Reports section.

When you run the report, you will be prompted for the parameter value(s) that correspond to the parameter(s) you have defined. For example, you can enter d% to get usernames starting with the letter d if you have defined a username parameter and written a corresponding SQL query.

Selecting Report Data

You can open the data dictionary to see the tables and column names that you can use in your reports. When you create a report, you open the Data Dictionary by clicking the >> button in the upper right area of the screen.

With the Data Dictionary visible, you can find the column names in a particular table by clicking the triangle next to a table name. The Data Dictionary provides table names, column names, and data types so that you know what to enter in your SQL query.

Although there are other tables in the database that you can use in your reports, the tables mentioned below are likely to be the most useful to you.

- **ADUser**: The Active Directory User table stores some basic information related to users, such as SamAccountName, UserPrincipalName, Mail, and so forth.
- **Application**: Stores information related to web and mobile applications, such as web application type, mobile application type, application version, and so forth.
- Device: Stores information related to mobile devices and Mac computers, such as operating system version, noncompliant status, and when the device last connected with the Privileged Access Service
- **Event**: Stores activity information related to applications, devices, and users, such as counts for application launches, logins, device types, and so forth.

Note: When creating queries with the Event table, you must specify a time boundary. There are too many records in the Event table to query all records. For details, see "Filtering events by time with DateFunc()".

Report Query Syntax

Creating the query for a report involves using SQL statements. SQL is a Structured Query Language for retrieving data from databases. SQL statements can be simple or complex, depending on the data that you want to find and how you want it to display. The key is to know what you want to see in your report, and understanding what kind of data is available to you.

For example, here's a simple SQL statement:

SELECT Owner FROM Device

This query looks for the listed owners of registered mobile devices, as recorded in the Owner column of the Device table.

The main component of a SQL query is the SELECT statement. SELECT does just that - it selects which data to display. You can select one or more columns from one or more tables to retrieve. You can use any of the following SELECT statements in Admin Portal report queries:

- SELECT: Selects data from the specified columns in the specified tables.
- SELECT *: Selects all records from the specified table.
- SELECT DISTINCT: Selects the unique records from the specified columns in the specified tables. The DISTINCT keyword trims out the duplicate records.

If you want to look at columns in different tables, you can also combine the results by using UNION or one of the JOIN statements.

In addition to selecting the database tables to retrieve, you can also provide conditions to further refine your query results. You can use any of the following SQL statements to specify conditions:

- AND / OR: Selects data that meets both conditions (AND) or one of the specified conditions (OR).
- BETWEEN: Use BETWEEN to select results that are within a specified range.
- IN / NOT IN: Use IN or NOT IN to specify multiple values in a WHERE clause.
- LIKE: Use LIKE to search for a specified pattern in a column.
- WHERE: Use WHERE to specify criteria to filter for, such as column values and so forth.

  Note: Admin Portal uses a subset of SQL-92 that only supports SELECT statements. SQL commands that change database values are not valid (CREATE, ALTER, DELETE, DROP, INSERT, SELECT INTO, TRUNCATE, UPDATE, and so forth).

Filtering Events by Time with DateFunc()

When you query the Event table, you must include a time boundary to limit your query results. Admin Portal provides a DateFunc() SQL function to filter events based on time.

The time span argument of DateFunc allows you to specify a combination of days, hours, minutes, and seconds. Its most generic form is:

'[-]d.hh:mm:s'

The leading '-' is optional. Days supports any number of digits, seconds supports 1 or 2 digits, and hours and minutes require 2 digits. It also supports the following forms so you don't have to use place holders for unneeded data:

Days: '[-]d' (equivalent to [-]d.00:00:00)

Hours/minutes: '[-]hh:mm' (equivalent to [-]0.hh:mm:00)

Hours/minutes/seconds" '[-]hh:mm:s' (equivalent to [-]0.hh:mm:s)

Examples of placeholders

- Last week: '-7'
- Next 2 hours: '02:00'
- Last 90 mins and 30 seconds: '-01:30:30'
- Last 7 days, 7 hours, 7 minutes, 7 seconds: '-7.07:07:7'

Description	SQL Query
Events that occurred in the last 30 days	select WhenOccurred, FailUserName, FromIPAddress from event where EventType = 'Cloud.Core.LoginFail' and whenoccurred >= DateFunc('now','-30')
Events that occurred in the last 24 hours	Select WhenOccurred,EventType from Event where WhenOccurred > datefunc('now', '-1')
Events that occurred in the last 48 hours	Select * from Event where WhenOccurred > DateFunc('now', '-2')
Events that occured in the last 54 hours	Select * from Event where WhenOccurred > DateFunc('now', '-2.06:00')
Events that occurred on or before August 7, 2013	select WhenOccurred, UserName, FromIPAddress, AuthMethod, Factors from Event where EventType = 'Cloud.Core.Login' and WhenOccurred > datefunc('now', -7)
Events that occurred yesterday	select eventtype,WhenOccurred from event where whenoccurred>datefunc('now', '-3') and whenoccurred < datefunc('now', '-2')

DateFunc Syntax

Use the following syntax:

DateFunc(<stringdate>, [<offset>])

where

<*stringdate*> can be one of the following three options:

- 'now' - this means now (current time)
- 'today' - this means the start of today (current day)

- <date string> - a string that represents a specific date and time, such as '09.30.2016:01:00'.

<*offset*> is a string representing an offset.

- -n means minus n days
- -5:00 means minus 5 hours

> **Note:** Privileged Access Service operates using UTC time and displays in local time. So, “today” means the start of today according to UTC time, and ‘3:15’ means 3:15 today in UTC time. For example, if you specify ‘3:15’ while you’re in California during Daylight Savings Time, you’re actually specifying 8:15 am UTC time.

Formatting Dates to Strings with Formatdate()

You can use the Formatdate() function to convert a date to a string. Use the following syntax:

formatdate(<date>, <format_string>)

For example, to extract the month number from a date, use the following syntax:

formatdate(<date>,”MM”)

If you process a date in November through the above example, it returns an “11” to indicate November.

Common Events that You Can Search For

When collecting information from the Event table, you specify types of events that you want to have in your report. Here’s a list of the most common types of events that you might see in the Event table.

Cloud.Saas.ApplicationLaunch

Cloud.Saas.Application.AppLaunch

Cloud.Saas.Application.AppAdd

Cloud.Saas.Application.AppModify

Cloud.Saas.Application.AppDelete

Cloud.Saas.Application.SamlResponseGenerate

Cloud.Saas.Application.WsFedSamlResponseGenerate

Cloud.Saas.ProfileUpdate

Cloud.Saas.PasswordChange

Cloud.Core.Login

Cloud.Core.Login.MultiFactorChallenge

Cloud.Core.Login.MultiFactorChallenge.MultiFactorResponse

Cloud.Core.LoginFail

Cloud.Core.Logout

Cloud.Core.SamlTokenValidate

Cloud.Core.SamlTokenValidateFail

Cloud.Core.Access.Role.Create

Cloud.Core.Access.Role.Edit

Cloud.Core.Access.Role.Delete

Cloud.Core.Access.CheckRightsFailure.Table

Cloud.Core.Access.CheckRightsFailure.Table.Row

Cloud.Mobile.Enroll

Cloud.Mobile.StateChange

Cloud.Mobile.AppChange

Cloud.Mobile.DeviceAction

Cloud.Mobile.Device.DeviceAction

Cloud.Mobile.Device.AppChange

Cloud.Mobile.Device.StateChange

Cloud.Mobile.Device.Enroll

Cloud.Mobile.GpChangeDetected

Working with Reports

When you open a report, use the **Actions** menu to invoke the following commands:

Action menu command	To do this
Run	Run a new report with a different set of parameters.
Add To Set	Adds the report to the specified set.
Modify >**Note**: The option name will be **Details** for built-in reports.	Display the reports details and set the following properties: Report can be displayed on a map Validate report on save The details include the report name, description, and SQL query. You can generate a preview of the results in this option too.
Email Report	Send the query results to an email account. You can send the data as an Excel spreadsheet or HTML table.
Export Report	Save the SQL script in a CSV or Excel spreadsheet file.
Copy	Copy the report.

Viewing Reports

When viewing a report, you can click any column heading to sort by that column. You can also click and drag a column heading to move it and adjust the column widths.

To view a report:

1. On the Reports page, select a report to open it.
2. Choose the parameters you want to use for your report.
3. Your report information will display once the parameters window closes.

Modifying Applications or Devices Directly from a Report

If your report includes web applications or devices in the report results, you can click a specific application or device to see the details for that object. This works when a specific object (device ID or application name) displays in the result set, not a grouping of objects.

For example, if you create a report that lists a mobile device ID, you can right-click the Device ID and perform device-related actions - such as delete, update policies, unregister, and so forth.

Exporting Report Data

You can export reports to a CSV or Microsoft Excel file.

To export a report

1. From **Reports**, open a report that you want to export.
2. Click **Actions > Export Report**.
3. Choose a file type and enter a filename, then click **OK**.

How to Create a new Report

You can create new reports using SQL and parameters. Using parameters in your SQL query allows you to run the same report against different values instead of creating multiple reports.

To create a new report:

1. Log in to Admin Portal.
2. Click **Reports** > **New Report**.
3. Enter a name for your report.

   Names can contain letters, numbers, and underscores. Do not include special characters or white space.
4. Use the Data Dictionary column drop-downs to define what you want the report to display.

   The data dictionary has a list of all tables. After you select a column, tables not valid for a join are automatically disabled. If more than two tables are joined, and one table no longer has any filters and columns, then only tables that can be joined together will remain selected and in the SQL. For example, if A is joined to B is joined to C, and B is removed, and A and C cannot be joined, then only A will remain in the SQL.

   You can click the filter icon associated with each column to specify conditions for filtering on that column. Only the IN and NOT IN operations allows for multiple values.
5. (Optional) Use the script editor to manually build your report.

   See "Report Query Syntax" for help with syntax.

   Write SQL queries that use parameters for arguments rather than concrete values. This will allow you to run the same report against different values. For example, you can write the following SQL query:

select username, lastlogin from user where username like @userParam

You now must define the “userParam” parameter to make use of the query.

6. Click **Parameters** to specify parameters.

   Parameters allow you to define a report with different values. Parameters you specify must be paired with your SQL query. In our example, the SQL query in the above step uses the “userParam” parameter, so you must define the same parameter here.

7. Click **Settings** to configure the report options:
   - Reports can be displayed on a map -- Enable this option to display the data on a map if the report is location related.
   - Validate reports on save (enabled by default) -- Enable this option to validate the SQL syntax when you save the report.

8. Click **Save**.

   Admin Portal saves your report to the Reports section.

When you run the report, you will be prompted for the parameter value(s) that correspond to the parameter(s) you have defined. For example, you can enter d% to get usernames starting with the letter d if you have defined a username parameter and written a corresponding SQL query.

Copying an Existing Report

To copy an existing report:

1. Open the **Reports** page.
2. Right-click the desired report and click **Copy**.
3. In the confirmation dialog box, click **Yes**.

   Note: You can copy any report you have access to.

4. Admin Portal saves a copy of the report with the same name appended with (Copy - DateTime).

Deleting a Report

You can delete a report from the Reports section.

To delete a report:

1. Right-click the desired report and click **Delete**.
2. In the confirmation dialog box, click **Yes**.

   Admin Portal deletes the specified report.

Viewing Device Attributes in Report Builder

When you create a dynamic set of endpoints, you can use attributes from the Device list in Report Builder.

To view the Device attribute list in Report Builder

1. In the Admin Portal, navigate to the Report Builder by clicking **Reports**.
2. Open an existing report and click **Actions > Details** or click **New Report** to start a new report.
3. In the Data Dictionary pane, click **Device** to expand the attribute list.

For more information on creating dynamic sets, see How to use sets to manage endpoints.

Policy-Updating Device Attributes

A subset of the Device attributes list has a unique behavior. If you use one of following attributes in a query and, subsequently, the value of that attribute changes, this will cause the device policy to update, automatically:

- Carrier
- IsAdminLocationTrackingEnabled
- Jailbroken
- Name
- OSBuild
- Owner
- OwnerID
- PhoneNumber

Report query examples: Built-in Report Definitions

Admin Portal provides some built-in reports that you can use or copy and then modify as desired. You can view the SQL statements for any of the built-in reports in Admin Portal. For convenience, here are some examples of the report definitions for several of the built-in reports so you can see examples of the SQL syntax being used.

Report description	Query syntax
Web apps used the most often during the last 30 days	select ApplicationName as Name, count(*) as Count from Event where WhenOccurred >= DateFunc('now', '-30') and EventType='Cloud.Saas.Application.AppLaunch' group by name order by count desc
Web apps added and used in the last 30 days	select distinct ApplicationName from Event where eventtype='Cloud.Saas.Application.AppLaunch' and ApplicationName in (select applicationname from event where whenoccurred >datefunc('now','-30') and eventtype='Cloud.Saas.Application.AppAdd'
Web apps that weren't used in the last 30 days	select Name from application where DisplayName not in (select ApplicationName from Event where WhenOccurred >= DateFunc('now', '-30') and EventType='Cloud.Saas.Application.AppLaunch') and AppType = 'Web'
A listing of the different Android versions in use	select OSVersion,Count(*) as Count from device where InternalDeviceType = 'A' group by osversion order by count desc

Report description	Query syntax
Number of devices, organized by mobile carrier	select Carrier, count(*) as Count from device group by Carrier
Number of devices, organized by iOS, Mac, Android, and Windows	select case(InternalDeviceType) when 'I' then 'iOS' when 'M' then 'Mac' when 'A' then 'Android' when 'W' then 'Windows' end as Platform, Count(*) as Count from device group by InternalDeviceType order by Count desc","DisplayName":"DeviceByPlatform
A listing of the different iOS versions in use	select OSVersion,Count(*) as Count from device where InternalDeviceType = 'I' group by osversion order by count desc
All mobile apps, organized by the number of installations	select Name, Count(*) as Count from InstalledApp group by name order by count desc
Failed logins in the last 30 days	select WhenOccurred, FailUserName, FromIPAddress from event where EventType = 'Cloud.Core.LoginFail' and whenoccurred >= DateFunc('now','-30')
Users who haven't logged in during the last 30 days	select UserName, DisplayName, LastLogin from User where ID not in (select UserGUID from Event where EventType = 'Cloud.Core.Login' and WhenOccurred >= DateFunc ('now', '-30'))
The users who have logged in the most often during the past 30 days	select NormalizedUser as User, Count(*) as Count from Event where EventType = 'Cloud.Core.Login' and WhenOccurred >= DateFunc('now', '-30') group by User order by count desc

Report Syntax Examples

SQL Statements to Retrieve Data from Tables and Columns (basic)

SQL Statement	Syntax	Example Statement	Example Result or Description
SELECT	SELECT column_name(s) FROM table_name	select Name from application	Use SELECT to get the data in one or more columns of a table.
SELECT *	SELECT * FROM table_ name	select * from ADGroup	Use SELECT to get all records from a table.

SQL Statement	Syntax	Example Statement	Example Result or Description
SELECT DISTINCT	SELECT DISTINCT column_name(s) FROM table_name	select distinct ApplicationName from Event	Use SELECT DISTINCT to return just the values that are unique (distinct). Duplicate values are ignored.
UNION (ALL)	SELECT column_name(s) FROM table_name1 UNION SELECT column_name(s) FROM table_name2		Use the UNION statement to combine result sets of two or more SELECT statements. Only distinct values are returned. To return all values, including duplicate values, use UNION ALL.

SQL Components to Specify Conditions

SQL Statement	Syntax	Example Statement	Example Result or Description
AND / OR	SELECT column_name(s) FROM table_name WHERE condition AND|OR condition	select WhenOccurred, FailUserName, FromIPAddress from event where EventType = 'Cloud.Core.LoginFail' and whenoccurred >= DateFunc('now','-30')	Use AND to combine conditions - results display if the database record meets both conditions. Use OR to show results that meet either the first or second condition.
BETWEEN (advanced)	SELECT column_name(s) FROM table_name WHERE column_name BETWEEN value1 AND value2	select OSVersion,Count(*) as Count from device where InternalDeviceType = 'I' and OSVersion between '6' and '7' group by osversion order by count desc	Use BETWEEN to select results that are within a specified range.
IN / NOT IN	SELECT column_name(s) FROM table_name WHERE column_name IN (value1,value2,..)	select UserName, DisplayName, LastLogin from User where username not in (select NormalizedUser from Event where EventType = 'Cloud.Core.Login' and WhenOccurred >= DateFunc('now', '-30'))	Use IN to select results where a column name is one of a specified list of values (or not).

SQL Statement	Syntax	Example Statement	Example Result or Description
LIKE	SELECT column_ name(s) FROM table_name WHERE column_name LIKE pattern	Select * from Users where username like ‘j%’ returns all users whose names begin with J	Use LIKE to select results that match a specified pattern. Use s to indicate the pattern. Use % for zero or more characters, and use _ (underscore) for a single character.
CASE (WHEN... THEN, END)	CASE X WHEN W1 THEN T1 WHEN W2 THEN T2 ELSE T3 END To evaluate the base expression multiple times: CASE WHEN X=W1 THEN T1 WHEN X=W2 THEN T2 ELSE T3 END	SELECT CASE(InternalDeviceType) WHEN 'I' THEN 'iOS' WHEN 'M' THEN 'Mac' WHEN 'A' THEN 'Android' WHEN 'W' THEN 'Windows' END as Platform, Count(*) as Count from device GROUP BY InternalDeviceType ORDER BY Count desc	Use CASE when you want to do an if/then/else statement. You can specify to have the base expression evaluated once or multiple times.
WHERE	SELECT column_ name(s) FROM table_name WHERE column_name operator value	select ApplicationName as Name, count(*) as Count from Event where WhenOccurred >= DateFunc('now', '-30') and EventType='Cloud.Saas.Application.AppLaunch' group by name order by count desc	Use WHERE to specify the condition, such as a column name value.

SQL Components to Specify Sorting, Displaying, Grouping

SQL Statement	Syntax	Example Statement	Example Result or Description
AS (alias)	SELECT column_name AS column_ alias FROM table_name or SELECT column_name FROM table_name AS table_alias	select Carrier, count(*) as Count from device group by Carrier	Use AS if you want to provide a different label for a column in the report results.

SQL Statement	Syntax	Example Statement	Example Result or Description
GROUP BY	SELECT Carrier, count(*) AS Count from device GROUP BY Carrier	select Carrier, count(*) as Count from device group by Carrier	Use GROUP BY to organize the report results by a specified column value.
ORDER BY	SELECT column_name(s) FROM table_name ORDER BY column_name [ASC|DESC]	select Name, Count(*) as Count from InstalledApp group by name order by count desc	Use SORT BY to sort the report results by a specified column value.

SQL Function Examples

SQL Statement	Syntax	Example Statement	Example Result or Description
HAVING	SELECT column_ name, aggregate_ function(column_ name) FROM table_ name WHERE column_name operator value GROUP BY column_ name HAVING aggregate_function (column_name) operator value		Use HAVING to specify conditions when using SQL aggregate functions. (Use instead of WHERE for aggregate functions.)
AVG()	SELECT AVG (column_name) FROM table_name;		Use AVG() to calculate the average value of the non-null records in the specified column.

SQL Statement	Syntax	Example Statement	Example Result or Description
COUNT()	SELECT COUNT (column_name) FROM table_name;	select ApplicationName as Name, count(*) as Count from Event where WhenOccurred >= DateFunc('now', '-30') and EventType='Cloud.Saas.Application.AppLaunch' group by name order by count desc	COUNT (Column_name) returns the number of non-null values in the specified column. COUNT (*) returns the number of records in a table. COUNT (Distinct column_ name) returns the number of distinct values in the specified column.
MAX() MIN()	SELECT MAX (column_ name)FROM table_ name; SELECT MIN (column_ name)FROM table_ name;		Use MAX() to return the maximum value of all values in the group. use MIN() to return the minimum, non-null value of all values in the group. The results include null values only if there are no non-null values.

Running Reports to View Effective Rights

There are built-in Infrastructure reports that you can customize to view effective user rights based on the criteria in which you are interested. For example, you can generate a report of the permissions assigned to a user or role for a specified account, database, domain, secret, service, or system. Similarly, you can generate a report that lists all of the permissions associated with Privileged Access Service objects for a specific user or role. You can then export to a file with commaseparated values or email the report to others.

To create a report of effective rights for Privileged Access Services:

1. In the Admin Portal, click **Reports**.
2. Click **Effective Rights** to display the types of reports available.

- **For Role** reports list the effective rights for a selected role on different types of Privileged Access Service objects or all Privileged Access Service objects.
- **For User** reports list the effective rights for a selected user on different types of Privileged Access Service objects or all Privileged Access Service objects.
- **Role to Object** reports list the effective rights for a selected role on different types of Privileged Access Service objects.
- **User to Object** reports list the effective rights for a selected user on different types of Privileged Access Service objects.

3. Select the type of report, then select the type of Privileged Access Service object for which you want information.

   For example, to see a complete list of the permissions granted on all Privileged Access Service objects for the members of the IT-Admin1 role, you would:

   - Select **For Role** as the report type.
   - Select **Audit Admin** as the role for which you want the complete list of permissions.
   - Click **Select**.

   The results are displayed in a results table.

4. Click **Actions** to:
   - Run the report again
   - Add the report to a set
   - See or customize the report details
   - Email the report to someone else or to a distribution list.
   - Export the report to a file with comma-separated values
   - Copy the report

Viewing Dashboards

The Dashboard pages provide handy summaries and graphical representations of your Centrify PAS usage. The built-in dashboards provide summaries of the following information:

- **Applications:** application status, type, recent app launches, and a listing of application details
- **Overview:** systems, accounts, checkouts, logins, and active sessions
- **Resource Counts:** systems, databases, accounts, services, and users
- **Security Overview:** denied logins, denied access, MFA factors, locations, and login and self service types
- **User Logins:** user login counts, locations, MFA factors, user logins by location, and user logins by directory service

Use the drop-down menu to select the dashboard pages.

In the upper-right corner of each dashboard, you can choose the time frame – data from the last 7 days or 24 hours.

Troubleshooting

There are a few common errors you might see when using Privileged Access Service, particularly if you have set up a demonstration environment for evaluation and testing. This section describes the most common errors, how to check the cause of the error, and what you can do to prevent the error from occurring.

Enabling read-only access for Privileged Access Service support

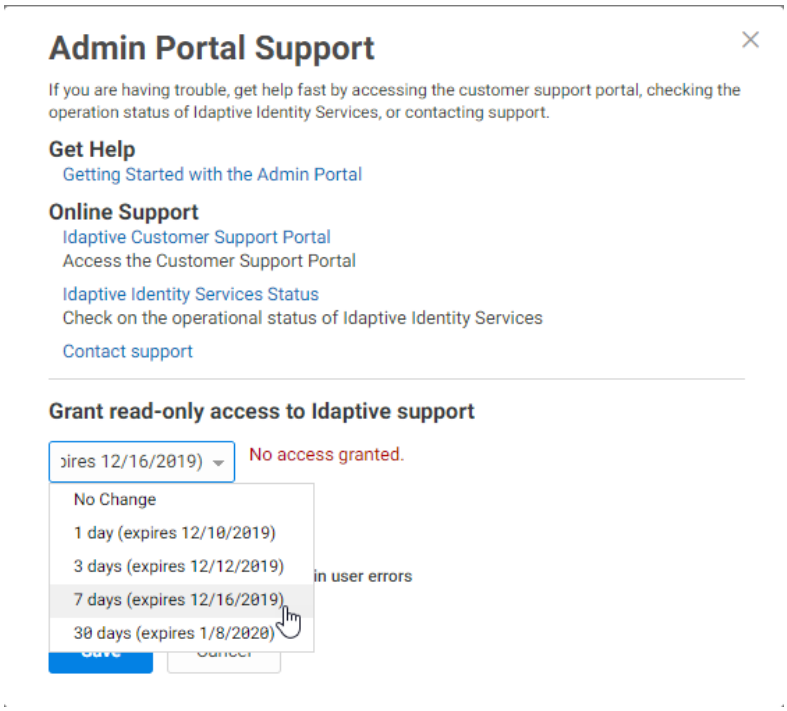
Sometimes, the best way to solve a problem is to grant Delinea support read-only access to your Privileged Access Service account.

Do not grant read-only access until you and your Delinea support technician agree that it is the best approach to solving your problem. You and the technician should also decide the appropriate time period before you grant access.

To enable read-only access for Delinea support

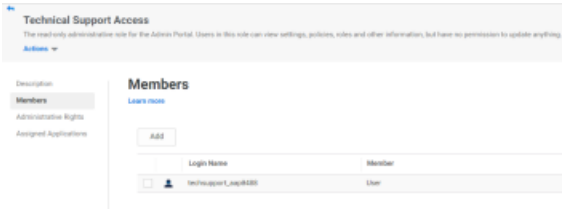
1. Log in to the Admin Portal.
2. Select the drop-down list next to your log-in account name, then click **Support**.

   The Admin Portal Support window opens.
3. Select the appropriate time period in the **Grant read-only access to Delinea support** drop-down list.



When you select a time period, Privileged Access Service automatically creates a Privileged Access Service user account named techsupport_aaannnnwhere aaannnn is your customer ID, creates a role named Technical SupportAccess with the Administrative Right Read Only Resource Management, and addsthe account to this

role. This is the account the support technician uses tolog in to your administrator portal. When the time period expires, this user account is locked and future attempted log-ins are blocked.

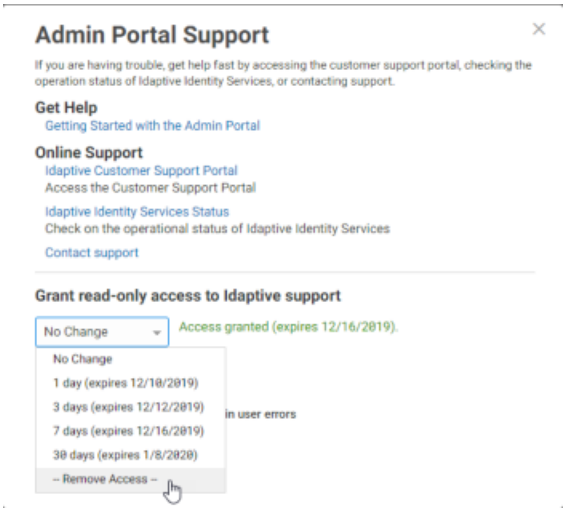


4. Click **Save**.

To revoke read-only access for Centrify support

1. Log in to the Admin Portal.
2. Select the drop-down list next to your log-in account name, then click **Support**.

   The Admin Portal Support window opens.
3. Select **-- Remove Access --** from the drop-down menu, then click **Save**.



The Privileged Access Service deletes the techsupport_aaannnn user account.

Adding Error Logging

You enable error logging to provide a detailed explanation when you receive an error message from the Privileged Access Service. Do not set this field unless you are repeatedly encountering a generic issue which requires you to contact Centrify support. The case is rare that you need to set this option. When you set the option, more detailed information is generated for the error message that you can pass on to the support technician.

To add error logging:

1. Log in to Admin Portal.
2. Select the drop-down list next to your log-in account name > select **Support**.

The Admin Portal Support window opens.

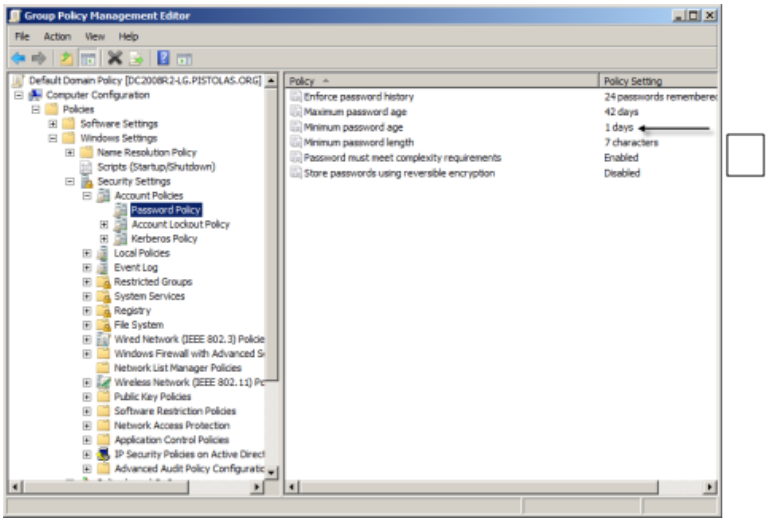
3. Select the check box associated with the **include diagnostic information in user errors** field.
4. Click **Save**.

Unable to update account password

If you attempt to add a local account to the privilege service and see the “Unable to update account password” error, it is most likely caused by the Minimum password age policy you have configured. It is common for organizations to configure to the Minimum password age policy to be 1 day. If you create a new local account for testing, then attempt to add the account and have its password managed by the privilege service, the service cannot update the password if the password fails the Minimum password age requirement.

To check the Minimum password age policy:

1. Open **Administrative Tools** and select **Group Policy Management**.
2. Select the **Default Domain Policy**, right-click, then select **Edit**.
3. Expand **Computer Configuration > Windows Settings > Security Settings > Account Policies**, then select **Password Policy**.
4. Check the **Minimum password age** setting.



If this policy is defined, you can either wait more than one day before adding the account with a password to be managed to the privilege service or you can disable the policy while testing with newly-created local accounts on computers joined to the domain. The issue doesn’t exist on computers that are not joined to the domain where the policy is set or for local accounts with a password exceeding the Minimum password age.

Privileged Access Service Integrations

Integration with Ansible

Delinea Privileged Access Service integrates with Ansible using playbooks and roles. Ansible automation for Delinea PAS is done by using:

Note: A minimum of Ansible AWX 18.0 is required to list Delinea Vault as a supported Credential.

How Ansible Works

Ansible is a radically simple IT automation engine that automates cloud provisioning, configuration management, application deployment, intra-service orchestration, and many other IT needs.

It has been designed for multi-tier deployments since day one. Ansible models your IT infrastructure by describing how all of your systems interrelate, rather than just managing one system at a time.

It uses no agents and no additional custom security infrastructure, so it's easy to deploy. Most importantly, it uses a very simple language (YAML, in the form of Ansible Playbooks) that enables you to describe your automation jobs in a way that is similar to plain English.

For more information, reference docs.ansible.com.

Efficient Architecture

Ansible connects to your nodes and pushes out small programs to them. These programs are called Ansible modules, and are written to be resource models of the desired system state. Ansible then executes these modules (over SSH by default), and removes them when finished.

Your library of modules can reside on any machine. No servers, daemons, or databases are required. Typically you'll work with your favorite terminal program, a text editor, and probably a version control system to keep track of content changes.

SSH Keys

Passwords are supported, but SSH keys with ssh-agent are one of the best ways to use Ansible. If you want to use Kerberos, that's good too; there are lots of options.

Note: Root logins are not required. You can login as any user, and then su or sudo to any user.

Ansible's **authorized_key** module is a great way to control which machines can access which hosts. Other options, like Kerberos or identity management systems, can also be used.

```
ssh-agent bash
ssh-add ~/.ssh/id_rsa
```

Manage Your Inventory in Simple Text Files

By default, Ansible represents what machines it manages using a very simple .ini file that puts all your managed machines in groups that you choose.

To add new machines, no additional SSL signing server is involved, so there's never a hassle in deciding why a particular machine didn't get linked up due to obscure NTP or DNS issues.

If there's another root source in your infrastructure, Ansible can also plugin to that. For example, a drawing inventory, group, and variable information from sources like EC2, Rackspace, OpenStack, and more.

Here's an example of a plain text inventory file:

```
[webservers]
www1.example.com
www2.example.com
[dbservers]
db0.example.com
db1.example.com
```

Once inventory hosts are listed, variables can be assigned to them in simple text files (in a subdirectory called **group_vars/ or host_vars/)** or directly in the inventory file.

Or, as previously mentioned, use a dynamic inventory to pull your inventory from data sources like EC2, Rackspace, or OpenStack.

Using Ansible For Ad Hoc Parallel Task Execution

Once you have an instance available, you can talk to it right away without any additional setup:

```
ansible all -m ping
ansible foo.example.com -m yum -a "name=httpd state=installed"
ansible foo.example.com -a "/usr/sbin/reboot"
```

Note: We have access to state-based resource modules as well as running raw commands. These modules are extremely easy to write, and Ansible ships with a fleet of them so most of your work is already done.

Note: Ansible contains a giant toolbox of over 750 built-in modules.

Using Playbooks

Playbooks can finely orchestrate multiple slices of your infrastructure topology, giving you very detailed control over how many machines to tackle at a time.

Ansible's approach to orchestration is one of finely-tuned simplicity. Your automation code should make perfect sense to you years down the road and there should be very little to remember about special syntax or features.

Here's what a playbook looks like:

Note: This example is just a teaser. See docs.ansible.com for the complete documentation and more in-depth playbook examples.

```
---
- hosts: webservers
serial: 5 # update 5 machines at a time
roles:
- common
- webapp
- hosts: content_servers
roles:
- common
- content
```

An example app_config.yml might look like:

```
---
- yum: name={{contact.item}} state=installed
with_items:
- app_server
- acme_software
- service: name=app_server state=running enabled=yes
- template: src=/opt/code/templates/foo.j2 dest=/etc/foo.conf
notify:
- restart app server
```

The Ansible documentation explores this in much greater depth. There's a lot more that you can do, including:

- Take machines in and out of load balancers and monitoring windows.
- Have one server know the IP address of all the other servers, using facts gathered about those servers, and using them to dynamically build out configuration files.
- Set variables, prompt for variables, and set default values for variables.
- Use the result of one command to determine whether to run another command.

There are lots of advanced possibilities but it's easy to get started.

Most importantly, the language remains readable and transparent, and you never have to declare explicit ordering relationships or write code in a particular programming language.

Extend Ansible: Modules, Plugins and API

If you want to write your own extensions, Ansible modules can be written in any language that can return JSON. For example, Ruby, Python, bash, etc.

Inventory can also plug into any data-source by writing a program that speaks to that data-source and returns JSON. There are also various Python APIs for:

- Extending Ansible connection types (SSH is not the only transport possible)
- Extending Ansible call-backs (how Ansible logs, etc)
- Adding server-side behaviors.

Create a Credential in Ansible AWX

1. Login as an Administrator to the AWX Portal
2. Navigate to **Resources** > **Credentials** and click on the **Add** button.
3. Set the **Name** for the Credential profile. For example Delinea Vault.
4. Set the **Credential type** to Delinea Vault Credential Provider Lookup.
5. Enter your **Delinea tenant URL**. For example https://abc1234.my.centrify.net
6. Enter the name of the **Delinea Service User** created earlier, For example ansible@mycompany.com where mycompany.com is the login suffix of the Service User.
7. Enter the password of the **Delinea Service User** created earlier.
8. Click on the **Test** button to validate the Credential profile.
9. The test will prompt you for the following:
   a. Account name for the credential checkout from the Vault.
   b. Name of the system this account is registered on. For example, root on server1234.
10. Save the **Credential Profile** after the test is complete.

Using Delinea Playbooks for Ansible

Installing Ansible

Ansible is widely available on Linux OS and can be installed using the Yum command on all RedHat type distributions. You can also use Ansible on additional distributions. For more information on additional distributions, refer to Ansible documentation .

Enabling Windows Management with Ansible

Ansible is used to manage Windows systems using PowerShell commands and command lines over WinRM.

- To enable Windows management by using the Ansible “winrm” module, install the Python module as documented by Ansible.
- For details on enabling Windows management with Ansible, refer to Ansible documentation.

Preparing for Delinea Automation

Automation includes unattended silent installation and bypassing password type credentials reserved for interactive authentication. Delinea recommends the following practice for silent installation and automated management:

- Delinea software deployment on Unix and Linux is supported using Delinea repository which can be addressed publicly (or mirrored if you are planning to use it for deployment onto systems that cannot access the Internet).
- For Active Directory management operation, Delinea recommends using a privileged service account and to maintain a Kerberos keytab file to avoid using password authentication.
- For Delinea Identity Platform Management operation, Delinea recommends using registration codes for system enrollment and OAuth2 protocol for REST API calls.

Configuring Delinea Repo

Ansible is used to manage the repository configuration (included into the sample Playbooks below). The Delinea repo should be configured first on your Ansible server using the appropriate configuration based on your Linux distribution. The setup example below shows how to setup a Yum repository assuming that the Ansible server is using RedHat Enterprise Linux or a RedHat derivative distribution (example: CentOS, Fedora, etc.).

Setup example using Yum repo:

1. Obtain your repo key, by following instructions in the Delinea Customer Portal.
2. Setup the repo by creating /etc/yum.repos.d/centrify.repo:

```
[centrify]
                name=centrify
                baseurl=https://username:password@repo.centrify.com/rpm-redhat/
                enabled=1
                repo_gpgcheck=1
                gpgcheck=1
                gpgkey=https://downloads.centrify.com/products/RPM-GPG-KEY-centrify
```

3. Verify proper operation

```
                $ sudo yum list Centrify*
                $ sudo yum info CentrifyDC

                centrify
                Available Packages
                Name        : CentrifyDC
                Arch        : i386
                Version     : 5.3.1
                Release     : 324
                Size        : 24 M
                Repo        : centrify
                Summary     : Centrify DirectControl Agent
                URL         : http://www.centrify.com/
```

For more details on all Centrify repos available, login to the Delinea Customer Portal and visit https://support.delinea.com/s/.

Configuring the Service Account Kerberos Secret

To join servers to the Active Directory using the Delinea agent requires privileged authentication to create or update data in the Active Directory domain. Delinea adjoin command support three different methods to perform the administrative operations in Active Directory:

- **Interactive authentication**, using an Active Directory privileged user principal and providing credentials when prompted. This option is ideal for a manual join. Any automation scenario would use either options below instead, as they do not require password disclosure.
- **Kerberos authentication**, using Kerberos ticket-granting-ticket of a privileged service account. In order to obtain a Kerberos ticket-granting-ticket for a service account principal, Delinea recommends using a Kerberos secret commonly named a keytab file (short for “key table”). A keytab is a file containing pairs of Kerberos principals and encrypted keys (which are derived from the Kerberos password). You can use a keytab file to authenticate to various remote systems using Kerberos without entering a password. However, when you change your Kerberos password, you will need to recreate all your keytabs. Keytab files are commonly used to allow scripts to automatically authenticate using Kerberos, without requiring human interaction or access to password stored in a plain-text file. The script is then able to use the acquired credentials to access files stored on a remote system.
- **Self-service authentication**, using a pre-created computer account in Active Directory.

Creating a Kerberos secret named /etc/adjoin.keytab for service account:

```
[root@lnx-prodapp01 ~]# adkeytab --keytab /etc/adjoin.keytab --user admin-cathy@domain.com
--adopt svc_centrifyadjoin
admin-cathy@DOMAIN.COM's password:
Success: Adopt Account: svc_centrifyadjoin
[root@lnx-prodapp01 ~]# ls -l /etc/adjoin.keytab
-rw-------. 1 root root 237 Mar 18 09:42 /etc/adjoin.keytab
 |
```

Note: The user specified to adopt the service account must be a privileged Active Directory user with permissions to change the password of the targeted service account. Service Account should be granted permissions to join computers to zones, remove computers from zones, and manage computer passwords.

You can verify the keytab file by listing the Keylist (Principals) using the Kerberos utility tool.

```
[root@lnx-prodapp01 ~]# ktutil
ktutil:  read_kt /etc/adjoin.keytab
ktutil:  list
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
1    3          svc_centrifyadjoin@DOMAIN.COM
2    3          svc_centrifyadjoin@DOMAIN.COM
3    3          svc_centrifyadjoin@DOMAIN.COM
```

```
ktutil:  quit
```

As a final verification, use the keytab file to obtain a Kerberos ticket-granting-ticket for the service account principal.

```
[root@lnx-prodapp01 ~]# kinit -kt /etc/adjoin.keytab svc_centrifyadjoin@DOMAIN.COM
[root@lnx-prodapp01 ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: svc_centrifyadjoin@DOMAIN.COM
Valid starting     Expires            Service principal
18/03/20 11:20:51  18/03/20 21:20:51  krbtgt/DOMAIN.COM@DOMAIN.COM
renew until 19/03/20 11:20:51
```

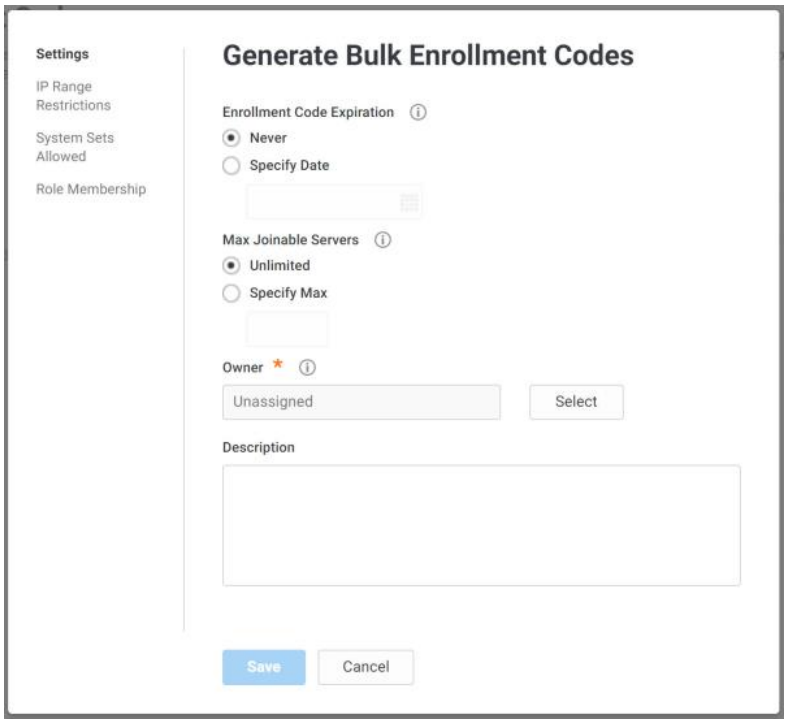
Note: For the **adjoin** command to be able to validate the **krbtgt** for kerberised join, you must edit the Kerberos configuration file **(/etc/krb5.conf)** to list the Kerberos realm (Active Directory domain) to use.

Creating a Registration Code

To allow unattended enrollment of systems into the Delinea Identity Platform, create a registration code that will be used to authenticate and allow the enrollment of a system when using the cenroll command from the Delinea Client or a custom script using REST API.

Creating a registration code in Delinea Privileged Access Service portal:

1. Login to the Delinea Privileged Access Service portal with an account member of System Administrators Role.
2. Navigate to **Settings** > **Enrollment** > **Enrollment Codes** then click on **Add** button.
3. On the **Settings** tab, choose a Delinea Role as owner of this registration code.



4. On the **IP Range Restrictions** tab, it is recommended to list the public IP from which you will allow this code to be used (or internal IP and ranges if using a customer managed PAS installation instead of a Delinea Cloud tenant).
5. On the **System Sets Allowed** tab, you can restrict the list of System Sets you allow the system to be added upon enrollment.
6. After saving the registration code, you will be invited to copy the generated code for future use (you can view the registration code again any time by selecting an existing code and **Actions**).

> **Note:** The registration code can be limited in time by setting an expiration or a number of systems to be enrolled before expiration. You can create more than one registration codes at any time, which can help delegation of multiple environment. Owner of a registration code will have permissions automatically set on systems enrolled using the registration code.

Using Delinea Automation Playbooks

You can manage Delinea agent deployment thanks to Delinea public repository available for all Delinea Privilege Services customers. Below are examples of playbooks for simple Delinea agents management tasks. These examples use Yum assuming that managed servers are using RedHat Enterprise Linux or a RedHat derivative distributions (CentOS, Fedora, etc.). Feel free to edit those examples to support other platforms and package management solution (for example, you may prefer to use Aptitude on Debian and derivative distributions).

You can also combine those playbooks into shorter or longer lists of tasks according to your needs, as you may want to perform installation and Active Directory in one single playbook or add Delinea agent deployment to existing orchestration flow. Finally, and depending of your needs, you may want to add more error handling to make those playbooks fully idempotent in your environment.

Delinea Agents Installation Playbook

The playbook below performs the following tasks:

- Create the configuration file for the Delinea repository if not already present.
- Install CentrifyDC and CentrifyDA packages using Yum.

Playbook example installing Delinea **agents:**

```
---
- hosts: all
become: true
vars:
centrify_repo: /etc/yum.repos.d/centrify.repo
tasks:
- name: Check if centrify.repo exists
stat:
path: "{{centrify_repo}}"
register: filecheck
- name: Create centrify.repo if it doesn't exist
copy:
src: "{{centrify_repo}}"
dest: "{{centrify_repo}}"
owner: root
group: root
mode: '0644'
when: filecheck.stat.exists == false
- name: Install Centrify Agents packages
yum:
update_cache: yes
name:
- CentrifyDC
- CentrifyDA
state: latest
```

Using Delinea Agents Uninstall Playbook

The playbook below performs the following tasks:

- Check if CentrifyDC package is installed (skip further actions if not installed).
- Check if computer is joined to domain (skip further actions if not joined).
- Uninstall CentrifyDC and CentrifyDA packages using Yum.

Playbook example uninstalling Delinea **Agents:**

```
---
- hosts: all
become: true
vars:
```

```
centrify_repo: /etc/yum.repos.d/centrify.repo
tasks:
- name: Check if CentrifyDC is installed
yum:
list: 'CentrifyDC'
register: yum_cmd
- name: Check if computer is joined to domain
command: adinfo
register: adinfo_cmd
changed_when: adinfo_cmd.rc == 10
failed_when: adinfo_cmd.rc != 10
- name: Remove Centrify Agents packages
block:
- name: Remove CentrifyDC, CentrifyDC-curl, CentrifyDC-openldap, CentrifyDC-openssl and
CentrifyDA packages
yum:
name: CentrifyDC
state: absent
- name: Delete centrify.repo
file:
path: "{{centrify_repo}}"
state: absent
when:
- yum_cmd.results | selectattr("yumstate", "match", "installed") | list | length == 1
- adinfo_cmd.rc == 10
```

Delinea Agents Activation Playbook

The playbook below performs the following tasks:

- Check if CentrifyDC package is installed (skip further actions if not installed).
- Check if computer is joined to domain (skip further actions if already joined).
- Copy Service Account keytab file for Kerberos join and obtain krbtgt.
- Join computer to domain using krbtgt.
- Destroy krbtgt and keytab file.

Playbook example running adjoin using Kerberos:

```
---
- hosts: all
become: true
vars:
domain_name: domain.com
user_principal: svc_centrifyadjoin@DOMAIN.COM
user_keytab: /etc/adjoin.keytab
container: domain.com/Centrify/Computers
zone: domain.com/Centrify/Zones/Global/Linux/Development
realm_config: /etc/krb5.conf
tasks:
```

```
- name: Check if CentrifyDC is installed
yum:
list: 'CentrifyDC'
register: yum_cmd
- name: Check if computer is joined to domain
command: adinfo
register: adinfo_cmd
changed_when: adinfo_cmd.rc == 10
failed_when:
- adinfo_cmd.rc != 10
- adinfo_cmd.rc != 0
- name: Join computer to Active Directory
block:
- name: Copy kerberos config file to guarantee finding realm
copy:
src: "{{realm_config}}"
dest: "{{realm_config}}"
owner: root
group: root
mode: '0644'
- name: Copy service account's keytab file
copy:
src: "{{user_keytab}}"
dest: "{{user_keytab}}"
owner: root
group: root
mode: '0600'
- name: Obtain service account's krbtgt
command: kinit -kt "{{user_keytab}}" "{{user_principal}}"
- name: Join the computer to Active Directory domain using kerberos
command: adjoin "{{domain_name}}" --container "{{container}}" --zone "{{zone}}" --verbose
- name: Destroy service account's krbtgt
command: kdestroy
- name: Securely remove service account's keytab file
command: shred --iterations=1 --remove "{{user_keytab}}"
when:
- yum_cmd.results | selectattr("yumstate", "match", "installed") | list | length == 1
- adinfo_cmd.rc == 10
```

The playbook below performs the following tasks:

- Check if CentrifyDC package is installed (skip further actions if not installed).
- Check if computer is joined to domain (skip further actions if already joined).
- Join computer to domain using self-service.

Playbook example running self-service adjoin:

```
---
- hosts: all
become: true
```

```
vars:
domain_name: domain.com
tasks:
- name: Check if CentrifyDC is installed
yum:
list: 'CentrifyDC'
register: yum_cmd
- name: Check if computer is joined to domain
command: adinfo
register: adinfo_cmd
changed_when: adinfo_cmd.rc == 10
failed_when:
- adinfo_cmd.rc != 10
- adinfo_cmd.rc != 0
- name: Join computer to Active Directory
block:
- name: Join the computer to Active Directory domain using self-service
command: adjoin "{{domain_name}}" --selfserve --verbose
when:
- yum_cmd.results | selectattr("yumstate", "match", "installed") | list | length == 1
- adinfo_cmd.rc == 10
```

Note: Self-service join requires pre-creation of a computer account in Active Directory domain, a computer profile in the target Centrify zone and delegate permissions to this computer to join the domain with self-service. This can be done by running the “Prepare UNIX Computer” wizard from the Access Manager console or using the PowerShell cmdlet New-CdmManagedComputer.

Delinea Agents Deactivation Playbook

The playbook below performs the following tasks:

- Check if CentrifyDC package is installed (skip further actions if not installed).
- Check if computer is joined to domain (skip further actions if not joined).
- Copy Service Account keytab file for Kerberos join and obtain krbtgt.
- Remove computer from domain using krbtgt.
- Destroy krbtgt and keytab file.

Playbook example running adleave:using Kerberos

```
---
- hosts: all
become: true
vars:
user_principal: svc_centrifyadjoin@DOMAIN.COM
user_keytab: /etc/adjoin.keytab
tasks:
- name: Check if CentrifyDC is installed
yum:
```

```
list: 'CentrifyDC'
register: yum_cmd
- name: Check if computer is joined to domain
command: adinfo
register: adinfo_cmd
changed_when: adinfo_cmd.rc == 0
failed_when:
- adinfo_cmd.rc != 10
- adinfo_cmd.rc != 0
- name: Remove computer from Active Directory
block:
- name: Copy service account's keytab file
copy:
src: "{{user_keytab}}"
dest: "{{user_keytab}}"
owner: root
group: root
mode: '0600'
- name: Obtain service account's krbtgt
command: kinit -kt "{{user_keytab}}" "{{user_principal}}"
- name: Leave Active Directory domain
command: adleave --remove --verbose
- name: Destroy service account's krbtgt
command: kdestroy
- name: Securely remove service account's keytab file
command: shred --iterations=1 --remove "{{user_keytab}}"
when:
- yum_cmd.results | selectattr("yumstate", "match", "installed") | list | length == 1
- adinfo_cmd.rc == 0
```

Delinea Client Installation Playbook

The playbook below performs the following tasks:

- Create the configuration file for the Delinea repository if not already present.
- Install CentrifyCC package using Yum.

Playbook example installing Delinea Client:

```
---
- hosts: all
become: true
vars:
centrify_repo: /etc/yum.repos.d/centrify.repo
tasks:
- name: Check if centrify.repo exists
stat:
path: "{{centrify_repo}}"
register: filecheck
- name: Create centrify.repo if it doesn't exist
copy:
```

```
src: "{{centrify_repo}}"
dest: "{{centrify_repo}}"
owner: root
group: root
mode: '0644'
when: filecheck.stat.exists == false
- name: Install Centrify Agent package
yum:
update_cache: yes
name: CentrifyCC
state: latest
```

Delinea Client Uninstallation Playbook

The playbook below performs the following tasks:

- Check if CentrifyCC package is installed (skip further actions if not installed).
- Check if computer is enrolled with a Centrify tenant (skip further actions if not joined).
- Uninstall CentrifyCC packages using Yum.

Playbook example uninstalling Delinea Client:

```
---
- hosts: all
become: true
vars:
centrify_repo: /etc/yum.repos.d/centrify.repo
tasks:
- name: Check if CentrifyCC is installed
yum:
list: CentrifyCC
register: yum_cmd
- name: Check if computer is joined to Centrify Identity Platform
command: cinfo
register: cinfo_cmd
changed_when: cinfo_cmd.rc == 10
failed_when:
- cinfo_cmd.rc != 10
- cinfo_cmd.rc != 0
- name: Remove Centrify Client package
block:
- name: Remove CentrifyCC package
yum:
name: CentrifyCC
state: absent
- name: Delete centrify.repo
file:
path: "{{centrify_repo}}"
state: absent
when:
```

```
- yum_cmd.results | selectattr("yumstate", "match", "installed") | list | length == 1
- cinfo_cmd.rc == 10
```

Delinea Client Enrollment Playbook

The playbook below performs the following tasks:

- Check if CentrifyCC package is installed (skip further actions if not installed).
- Check if computer is enrolled to a Delinea tenant (skip further actions if already joined).
- Enroll computer to Delinea tenant using a registration code.
- Enroll and manage password for the root account.

Playbook example running cenroll using registration code:

```
---
- hosts: all
become: true
vars:
tenant: <YourTenant>.my.centrify.net
code: <RegistrationCode>
tasks:
- name: Check if CentrifyCC is installed
yum:
list: 'CentrifyCC'
register: yum_cmd
- name: Check if computer is enrolled to Centrify Identity Platform
command: cinfo
register: cinfo_cmd
changed_when: cinfo_cmd.rc == 10
failed_when:
- cinfo_cmd.rc != 10
- cinfo_cmd.rc != 0
- name: Enroll computer to Centrify Identity Platform
block:
- name: Enroll the computer to Centrify tenant using registration code
command: cenroll --tenant "{{tenant}}" --code "{{code}}" --features all --force --verbose
when:
- yum_cmd.results | selectattr("yumstate", "match", "installed") | list | length == 1
- cinfo_cmd.rc == 10
```

Delinea Client Unenrollment Playbook

The playbook below performs the following tasks:

- Check if CentrifyCC package is installed (skip further actions if not installed).
- Check if computer is enrolled to a Delinea tenant (skip further actions if not joined).
- Unenroll computer from Delinea tenant using machine credentials.

Playbook example running cunenroll:

```
---
- hosts: all
become: true
vars:
tenant: <YourTenant>.my.centrify.net
code: <RegistrationCode>
tasks:
- name: Check if CentrifyCC is installed
yum:
list: 'CentrifyCC'
register: yum_cmd
- name: Check if computer is enrolled to Centrify Identity Platform
command: cinfo
register: cinfo_cmd
changed_when: cinfo_cmd.rc == 10
failed_when:
- cinfo_cmd.rc != 10
- cinfo_cmd.rc != 0
- name: Enroll computer to Centrify Identity Platform
block:
- name: Enroll the computer to Centrify tenant using registration code
command: cenroll --tenant "{{tenant}}" --code "{{code}}" --features all --force --verbose
when:
- yum_cmd.results | selectattr("yumstate", "match", "installed") | list | length == 1
- cinfo_cmd.rc == 10
```

Using Delinea Roles for Ansible

The following details advanced directory structure as recommended by Ansible best practices. This includes Ansible roles for Delinea that allow you to deploy and configure components easily into your environment.

Advanced Directory Structure

The top level of the directory would contain files and directories similar to the following:

```
production            # inventory file for production servers
staging               # inventory file for staging servers

group_vars/
   group1.yml         # here assign variables to particular groups
   group2.yml
hosts_vars/
   hostname1.yml      # here assign variables to particular systems
   hostname2.yml

site.yml              # master playbook

roles/
   common/            # this hierarchy represent a “role”
      tasks/          #
         main.yml     # <-- tasks file can include smaller files
```

```
      handlers/       #
         main.yml     # <-- handlers file
      templates/      # <-- files for use with the template resource
         ntp.conf.j2  # <-- templates end in .j2 (Jinja2 notation)
      files/          # <-- files for use with the template resource
         bar.txt      # <-- files for use with the copy resource
         foo.sh       # <-- script files for use with the script resource
      vars/           #
         main.yml     # <-- variables associated with this role
      defaults/       #
         main.yml     # <-- default lower priority variables for this role
      library/        # roles can include custom modules
      module_utils/   # roles can also include custom module_utils
      lookup_plugins/ # or other types of plugins, like lookup in this case

  centrify_audit/     # role for Centrify Audit and Monitoring Services
  centrify_auth/      # role for Centrify Authentication and Privilege Elevation Services
  centrify_vault/     # role for Centrify Privileged Access Service
```

Note: There are alternative structures aiming to present inventory in a separate directory. This is particularly useful if your group_vars and host_vars don't have that much in common in different environments. More on this can be learned by consulting the Ansible documentation.

Master Playbook Example

```
---
- hosts: all
roles:
- centrify_vault
- centrify_auth
- centrify_audit
```

Delinea Audit Role

This Ansible role provides tasks and sample configuration file to deploy Delinea Audit agent and enable session auditing on target systems.

Directory structure

```
centrify_audit/
default/
main.yml    # default variables for Centrify Audit installation and enablement
tasks/
disable.yml # tasks for disabling Centrify Audit
enable.yml. # tasks for enabling Centrify Audit
install.yml # tasks for installation of the Centrify Audit agent
main.yml.   # tasks invoked when role is applied to system
remove.yml  # tasks for uninstallation of the Centrify Audit agent
```

Default variables sample

```
---
# file: roles/centrify_audit/default/main.yml
# Common variables
centrify_repo: /etc/yum.repos.d/centrify.repo

# Centrify Audit and Monitoring Services Variables
installation_name: <AuditInstallationName>
```

Delinea Authentication Role

This Ansible role provides tasks and sample configuration file to deploy Delinea Authentication and Privilege Elevation agent and join the target systems to Active Directory domain.

Directory structure

```
centrify_auth/
   default/
      main.yml              # default variables for Centrify Authentication Agent
installation and enablement
   files/
      adjoin.keytab         # Keytab file for Kerberos join to Active Directory
      Join-CentrifyZone.ps1 # PowerShell script to join Windows system to Centrify Zone
      debian.repo           # Repository file for Aptitude
      redhat.repo           # Repository file for Yum
      suse.repo             # Repository file for Zypper
      krb5.conf             # Kerberos realm configuration file for Active Directory
   tasks/
      Debian-enroll.yml     # Tasks enabling Centrify Agent on Debian OS family
      Debian-install.yml    # Tasks installation of Centrify Agent on Debian OS family
      Debian-remove.yml     # Tasks uninstallation of the Centrify Agent on Debian OS
family
      Debian-unenroll.yml   # Tasks disabling Centrify Agent on Debian OS family
      RedHat-enroll.yml     # Tasks enabling Centrify Agent on RedHat OS family
      RedHat-install.yml    # Tasks tasks for installation of Centrify Agent on RedHat OS
family
      RedHat-remove.yml     # Tasks uninstallation of the Centrify Agent on RedHat OS
family
      RedHat-unenroll.yml   # Tasks disabling Centrify Agent on RedHat OS family
      Suse-enroll.yml       # Tasks enabling Centrify Agent on SuSE OS family
      Suse-install.yml      # Tasks installation of Centrify Agent on SuSE OS family
      Suse-remove.yml       # Tasks uninstallation of the Centrify Agent on SuSE OS family
      Suse-unenroll.yml     # Tasks disabling Centrify Agent on SuSE OS family
      Windows-enroll.yml    # Tasks enabling Centrify Agent on Windows OS family
      Windows-install.yml   # Tasks installation of Centrify Agent on Windows OS family
      Windows-remove.yml    # Tasks uninstallation of the Centrify Agent on Windows OS
family
      Windows-unenroll.yml  # Tasks disabling Centrify Agent on Windows OS family
      main.yml.             # Tasks invoked when role is applied to system
```

Configuring Authentication Role

To start using this role, configure the default variables under **roles/centrify_auth/defaults/main.yml** or use them into Host_vars or Group_vars definition files. Generate or edit the following files under **roles/centrify_auth/files:**

```
| File | Action |
| ----- | ----- |
| adjoin.keytab | You can generate a keytab file to use with Active Directory service
account using the adkeytab commands on Linux (requires a <span class="global-
vars.CompanyName mc-variable">Delinea</span> joined Linux server). |
| <span class="global-vars.CompanyName mc-variable">Delinea</span> Agent for Windows64.msi
and Group Policy Deployment.mst | Both those files should be copied from the software
source of the <span class="global-vars.CompanyName mc-variable">Delinea</span>
Infrastructure Services for Windows in use. Those two files are located under /Agent
folder. |
| Join-CentrifyZone.ps1 | This PowerShell script is provided as example of how to join
Windows systems to existing Centrify Zone. This script can be modified to satisfy any
customization of the join process in your environment. |
| krb5.conf | You can copy the Kerberos config file of any of your <span class="global-
vars.CompanyName mc-variable">Delinea</span> joined Linux systems to the same Active
Directory domain you plan to join using Ansible. Alternatively, you can manually create
this file using Kerberos documentation. |
| debian.repo, redhat.repo, and suse.repo | These files are provided as a sample and are
using <span class="global-vars.CompanyName mc-variable">Delinea</span> public
repositories. You must edit and replace the user:password string with your Repo
Credentials that can be found from the <span class="global-vars.CompanyName mc-
variable">Delinea</span> Download Center after creation of a Repo Key. You may also
customize the information of the repo to point to an internal mirror in case systems
targeted by Ansible may not have Internet access. |
```

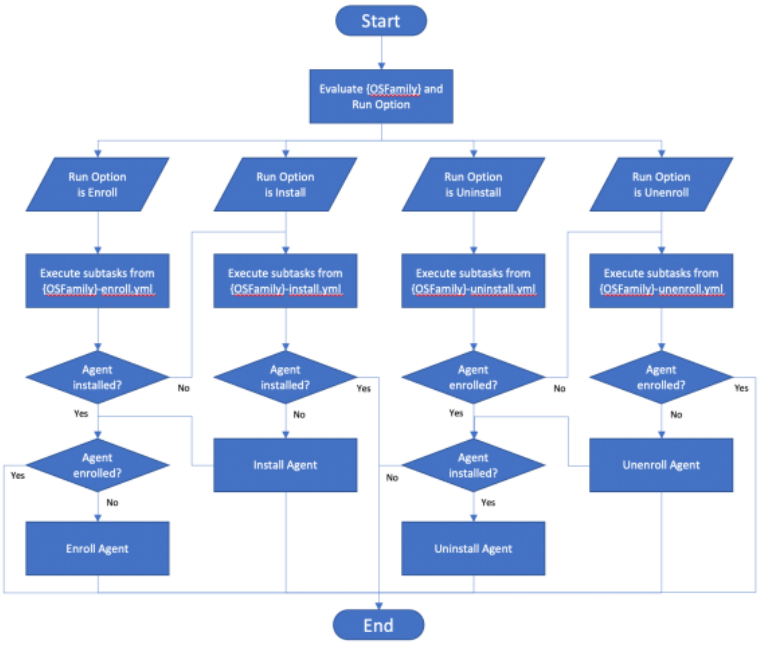
Default variables

```
---
## Common variables
# Default mode for running the playbook
# Possible values:
#  - install
#  - enroll
#  - unenroll
#  - remove
centrify_auth_run_option: enroll

# Repository configuration file to use on RedHat OS
# Default value:
#   centrify_auth_redhat_repo: /etc/yum.repos.d/centrify.repo
centrify_auth_redhat_repo: /etc/yum.repos.d/centrify.repo

# Repository configuration file and line to use on Debian OS
# Your Repo Credentials can be found from the Centrify Download Center after creation of a
Repo Key.
# You may also edit the information of the debian_repo_config to point to an internal
mirror in case systems targeted by Ansible may not have Internet access.
```

```
# Default values:
#   centrify_auth_debian_repo: /etc/apt/sources.list.d/centrify.list
centrify_auth_debian_repo: /etc/apt/sources.list.d/centrify.list

# Repository configuration file to use on SuSE OS
# Default value:
#   centrify_auth_suse_repo: /etc/zypp/repos.d/centrify-rpm-suse.repo
centrify_auth_suse_repo: /etc/zypp/repos.d/centrify-rpm-suse.repo

### Centrify Authentication and Privilege Elevation Services variables
# Active Directory domain name to use during join operations
# Example:
#   centrify_auth_domain: domain.com
centrify_auth_domain:

# Active Directory Service Account to use during join operations
# Example:
#   centrify_auth_service_principal: svc_centrifyadjoin@DOMAIN.COM
centrify_auth_service_principal:

# Location of the Kerberos Keytab file to use during join operations
# Default:
#   centrify_auth_service_keytab: /etc/adjoin.keytab
centrify_auth_service_keytab: /etc/adjoin.keytab

# Location of the Kerberos Realm configuration file to use during join operations
# Default:
#   centrify_auth_realm_config: /etc/krb5.conf
centrify_auth_realm_config: /etc/krb5.conf

# Active Directory container to use for Computers object during join operations
# Example:
#   centrify_auth_container: domain.com/Centrify/Computers
centrify_auth_container:

# Centrify Zone to use during join operations
# Example:
#   centrify_auth_zone: domain.com/Centrify/Zones/Global/Linux
centrify_auth_zone:
```

Executing Tasks

When applying this role to systems in a playbook execution, Ansible will call the main tasks definition file **roles/centrify_auth/tasks/main.yml** This file uses Ansible variables to invoke the corresponding sub tasks based on the OS family and run options as detailed below:



Configuring Custom Tasks

Tasks files can be edited to customize operations.

Delinea Vault Role

This Ansible role provides tasks and sample configuration file to deploy Delinea Client and enrol target systems to your Delinea Privileged Access Service tenant.

Directory structure

```
centrify_vault/
   default/
      main.yml              # default variables for Centrify Vault Client installation and
enablement
   files/
      debian.repo           # Repository file for Aptitude
      redhat.repo           # Repository file for Yum
      suse.repo             # Repository file for Zypper
   tasks/
      Debian-enroll.yml     # Tasks enabling Centrify Client on Debian OS family
      Debian-install.yml    # Tasks installation of Centrify Client on Debian OS family
      Debian-remove.yml     # Tasks uninstallation of the Centrify Client on Debian OS
family
      Debian-unenroll.yml   # Tasks disabling Centrify Client on Debian OS family
      RedHat-enroll.yml     # Tasks enabling Centrify Client on RedHat OS family
      RedHat-install.yml    # Tasks tasks for installation of Centrify Client on RedHat OS
family
      RedHat-remove.yml     # Tasks uninstallation of the Centrify Client on RedHat OS
family
```

```
      RedHat-unenroll.yml   # Tasks disabling Centrify Client on RedHat OS family
      Suse-enroll.yml       # Tasks enabling Centrify Client on SuSE OS family
      Suse-install.yml      # Tasks installation of Centrify Client on SuSE OS family
      Suse-remove.yml       # Tasks uninstallation of the Centrify Client on SuSE OS
family
      Suse-unenroll.yml     # Tasks disabling Centrify Client on SuSE OS family
      Windows-enroll.yml    # Tasks enabling Centrify Client on Windows OS family
      Windows-install.yml   # Tasks installation of Centrify Client on Windows OS family
      Windows-remove.yml    # Tasks uninstallation of the Centrify Client on Windows OS
family
      Windows-unenroll.yml  # Tasks disabling Centrify Client on Windows OS family
      main.yml.             # Tasks invoked when role is applied to system
```

Configuring the Vault Role

To start using this role, configure the default variables under **roles/centrify_vault/defaults/main.yml** or use them into Host_vars or Group_vars definition files. Generate or edit the following files under **roles/centrify_vault/files:**

```
| File | Action|
| ----- | ----- || ----- | ----- |
| debian.repo | |
| redhat.repo | |
| suse.repo | These files are provided as a sample and are using <span class="global-
vars.CompanyName mc-variable">Delinea</span> public repositories. You must edit and
replace the user:password string with your Repo Credentials that can be found from the
<span class="global-vars.CompanyName mc-variable">Delinea</span> Download Center after
creation of a Repo Key. You may also customize the information of the repo to point to an
internal mirror in case systems targeted by Ansible may not have Internet access. |
```

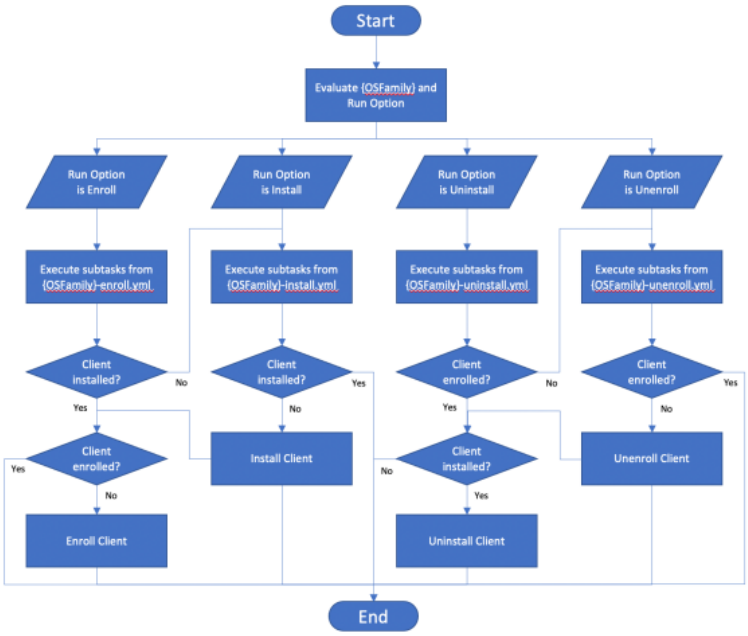
Default variables

```
---
## Common variables
# Default mode for running the playbook
# Possible values:
#  - install
#  - enroll
#  - unenroll
#  - remove
centrify_vault_run_option: enroll

# Repository configuration file to use on RedHat OS
# Default value:
#   centrify_vault_redhat_repo: /etc/yum.repos.d/centrify.repo
centrify_vault_redhat_repo: /etc/yum.repos.d/centrify.repo

# Repository configuration file and line to use on Debian OS
# Your Repo Credentials can be found from the Centrify Download Center after creation of a
Repo Key.
```

```
# You may also edit the information of the debian_repo_config to point to an internal
mirror in case systems targeted by Ansible may not have Internet access.
# Default values:
#   centrify_vault_debian_repo: /etc/apt/sources.list.d/centrify.list
centrify_vault_debian_repo: /etc/apt/sources.list.d/centrify.list

# Repository configuration file to use on SuSE OS
# Default value:
#   centrify_vault_suse_repo: /etc/zypp/repos.d/centrify-rpm-suse.repo
centrify_vault_suse_repo: /etc/zypp/repos.d/centrify-rpm-suse.repo

### Centrify Privileged Access Services variables
# Centrify PAS Platform tenant URL to use
# Example:
#   centrify_vault_tenant_url: https://company.my.centrify.net
centrify_vault_tenant_url:

# URL to use to download the Centrify Client for Windows from PAS Platform.
# This URL can be found on the Download section of the Centrify PAS Portal.
# Default:
#   centrify_vault_cagent_url: http://edge.centrify.com/products/cloud-
service/WindowsAgent/Centrify/cagentinstaller.msi
centrify_vault_cagent_url: http://edge.centrify.com/products/cloud-
service/WindowsAgent/Centrify/cagentinstaller.msi

# Registration code to use for Centrify Client enrolment to the Centrify PAS Platform.
# This code must be generated by a System Administrator under section Settings >
Enrollment > Enrollment Codes of the Centrify PAS Portal.
# Example:
#   centrify_vault_registration_code: 3JWTXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXC8W1
centrify_vault_registration_code:

# Feature to enable at enrollment
# Possible values:
#  - all
#  - agentauth
#  - aapm
#  - dmc
centrify_vault_features: all

# Enable Local Account Password Management for system account (i.e. root)
# Possible values:
#  - true
#  - false
centrify_vault_lapm: true

# Temporary password value used for enabling management of local account passwords.
# Note that this value will be immediately changed by the Centrify Vault and only used
once for the vaulting process.
# Example:
#   centrify_vault_tmp_password: T3mpOr4ryP4sswOrd!
centrify_vault_tmp_password: T3mpOr4ryP4sswOrd!
```

Executing Tasks

When applying this role to systems in a playbook execution, Ansible will call the main tasks definition file **roles/centrify_vault/tasks/main.yml**. This file uses Ansible variables to invoke the corresponding sub tasks based on the OS family and run options as detailed below:



Configuring Custom Tasks

The task file **roles/centrify_vault/tasks/post_enroll.yml** contains tasks performed after successful enrollment of the Delinea Client. This file is provided by default with few tasks commonly executed after enrollment, and can be customized to add any additional tasks relevant to your environment. Additionally, tasks files can be edited to customize operations.

Entra ID Integration with PAS/Cloud Suite

To integrate Cloud Suite/Privileged Access Service with Microsoft Entra ID Integration, review and perform the steps in the following sections:

- "Integration Prerequisites" on the next page
- "Setting Up Security Assertion Markup Language (SAML)" on the next page
- "Testing the Microsoft Azure Active Directory Integration" on page 1106

Note: At the end of 2023, Microsoft completed the change of their product name from Microsoft Azure Active Directory (Azure AD or ADD) to Microsoft Entra ID Integration (Entra or Entra ID).

Integration Prerequisites

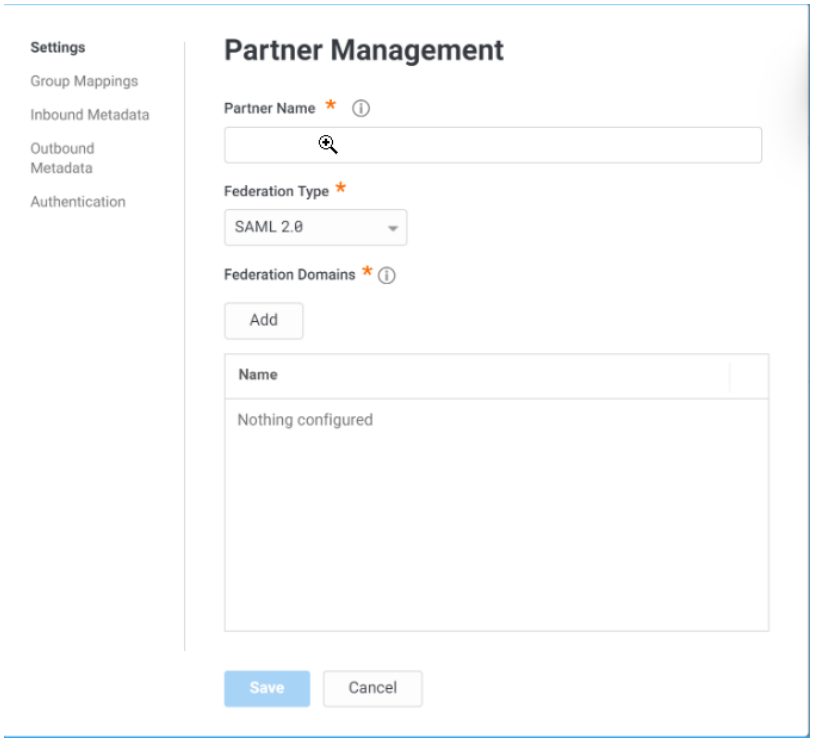
Before you begin the Delinea Privileged Access Service and Microsoft Azure Active Directory integration, ensure you have the following prepared in advance:

1. A Microsoft Azure Active Directory administrator account with permission to create SAML applications.
2. A Delinea PAS account with administrative permission (to create a partner).

Setting Up Security Assertion Markup Language (SAML)

To integrate Privileged Access Service and Microsoft Azure Active Directory, review and perform the following steps:

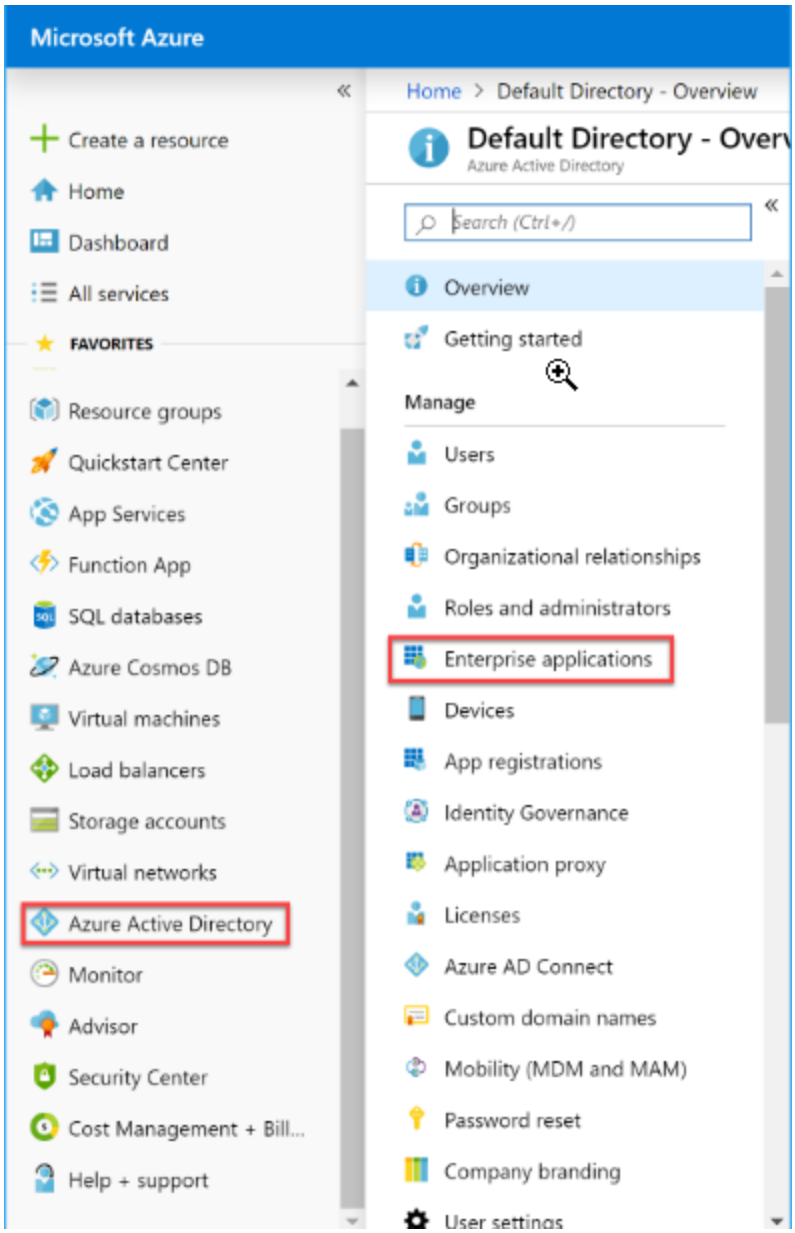
1. Open a browser tab or window to a {Company} PAS and navigate to **Settings** > **Users** > **Partner Management** and click **Add**.
2. On the main **Settings** tab, enter values in the following fields:



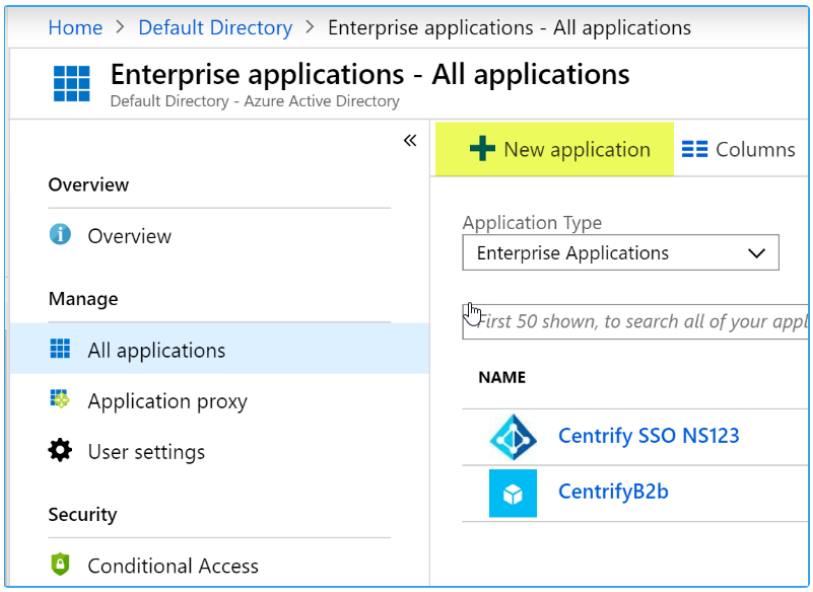
- **Partner Name** Azure.
- **Federation Type** SAML 2.0.
- Under **Federation Domains**, click **Add**, enter the domain for users and click **Add** again.

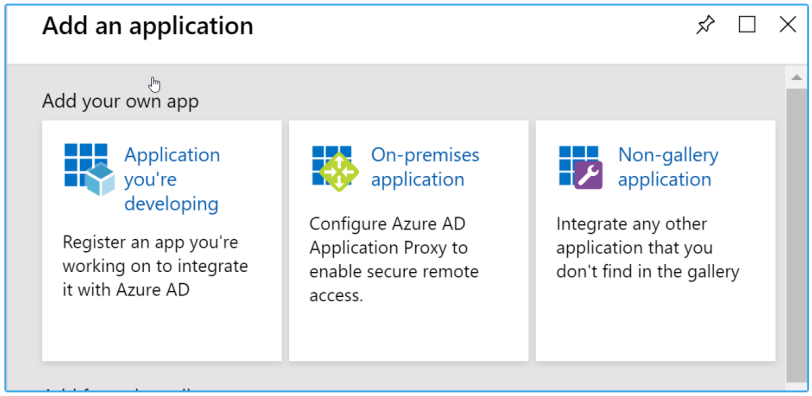
Note: You are about to pivot to the Microsoft Azure Active Directory. Do not close this window as you will return back to it to conclude set up.

3. Open another browser to log into Microsoft Azure Active Director (https://portal.azure.com) as an administrator to setup a new enterprise application that will federate with {Company}. Once you are in the main console click the **Azure Active Directory** service in the left-hand menu.

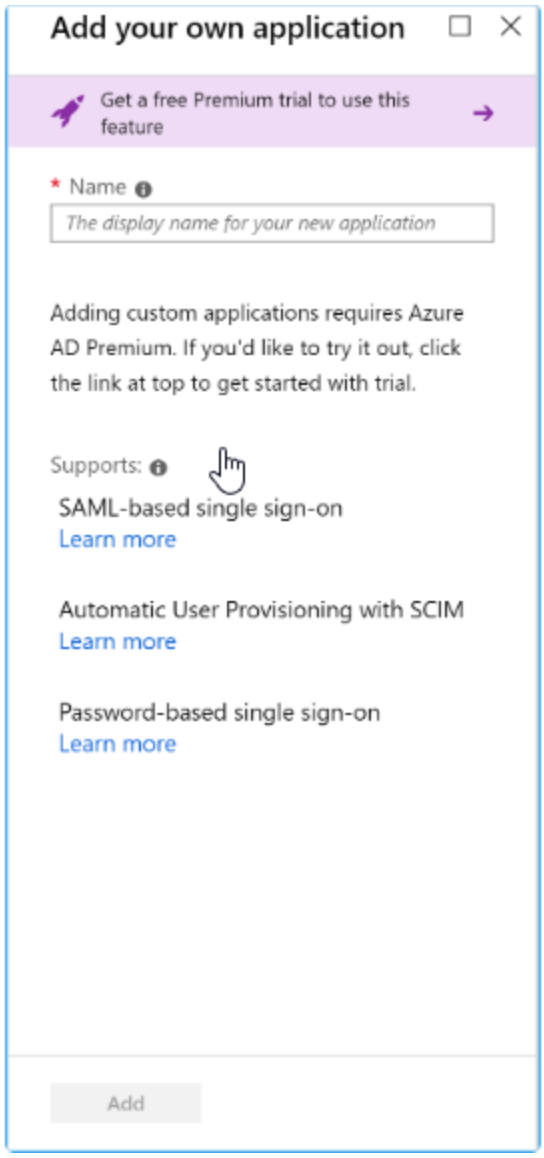


4. Click **New application** and make sure it is a **Non-gallery application.**

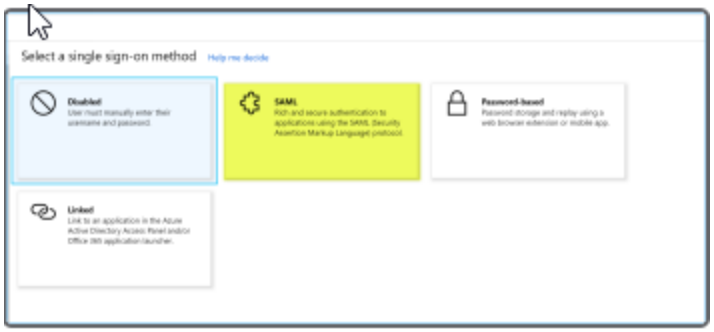




5. Name the application and **Add**.

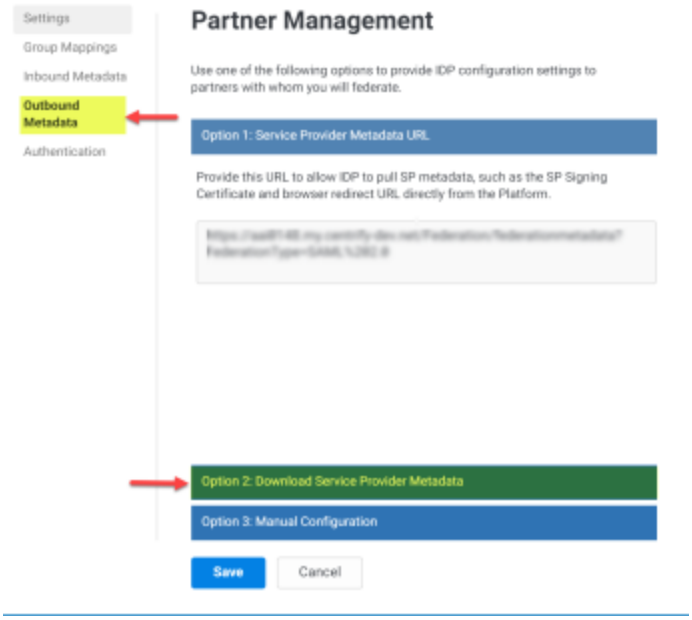


6. Select the **SAML** single sign-on method.

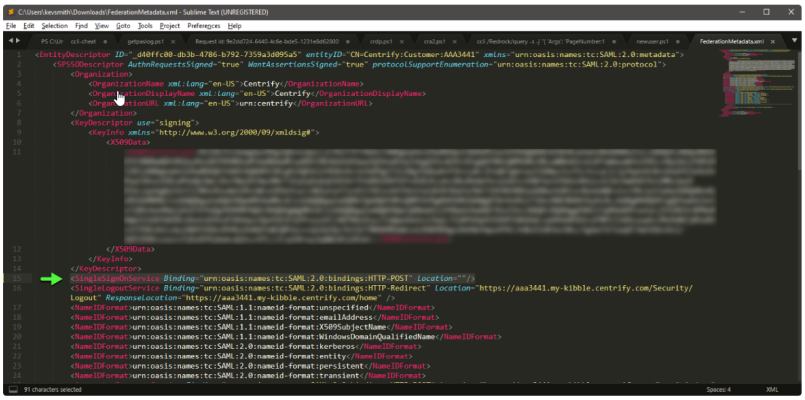


Note: This is a good time to bring back up the Delinea Partner add page you still have open.

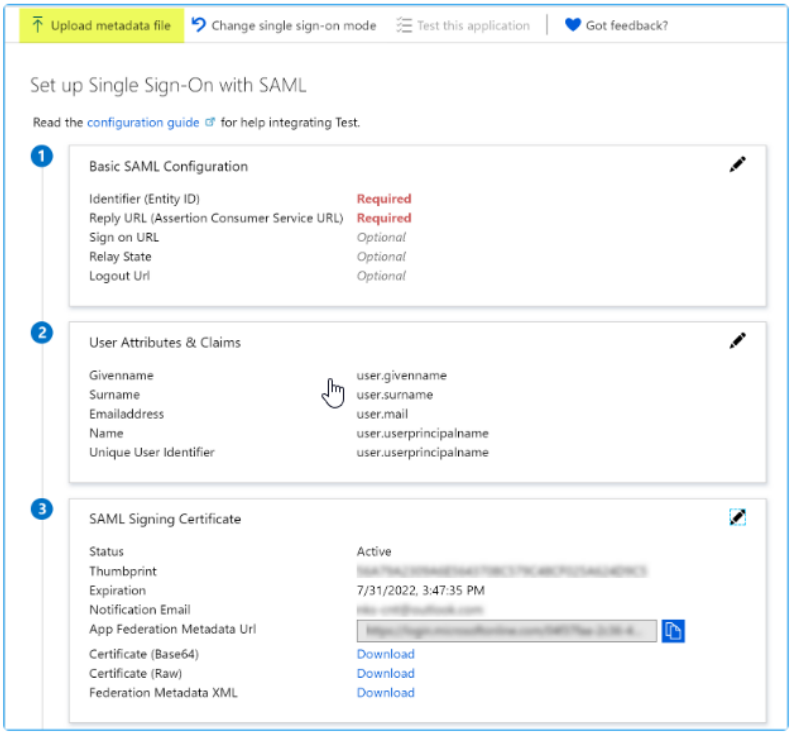
7. In the **Partner Management** window, select the **Outbound Metadata** tab and choose **Option 2: Download Service Provider Metadata**. Save the file to downloads or another location of choice.



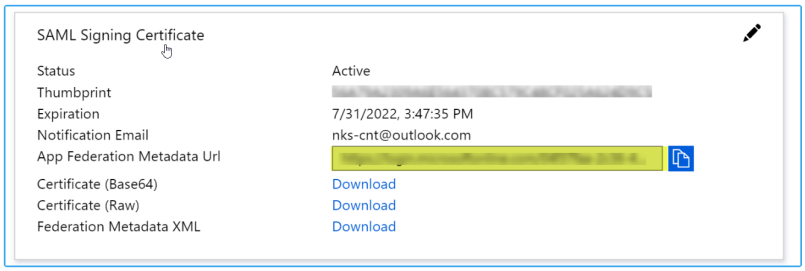
8. Edit the FederationMetadata.xml file by inserting the following line between </KeyDescriptor> and <SingleLogoutService> : <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location=""/>, as seen below:



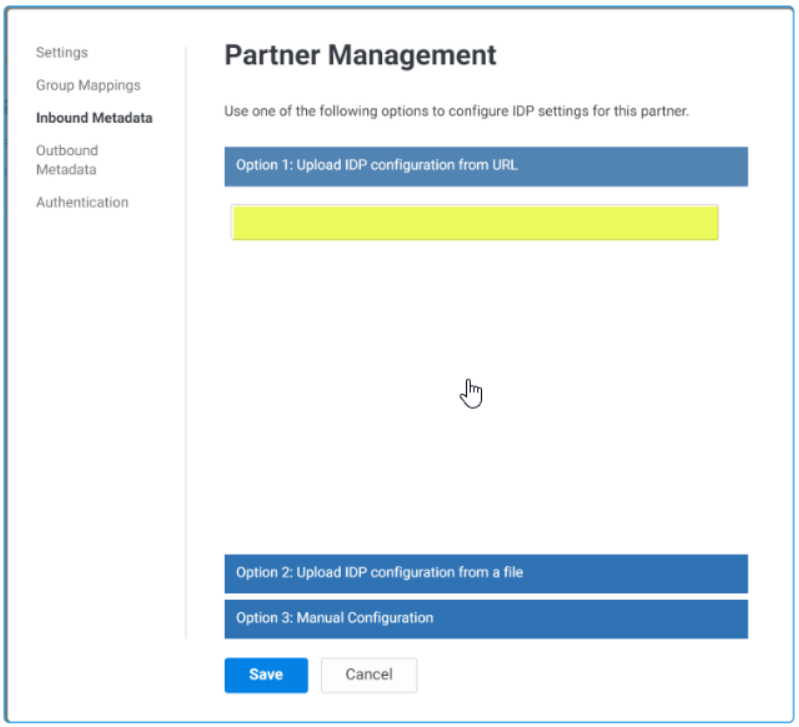
9. Save the file.
10. Go back to the Microsoft Azure Active Directory page, click **Upload metadata file** and upload the file you just downloaded and saved.



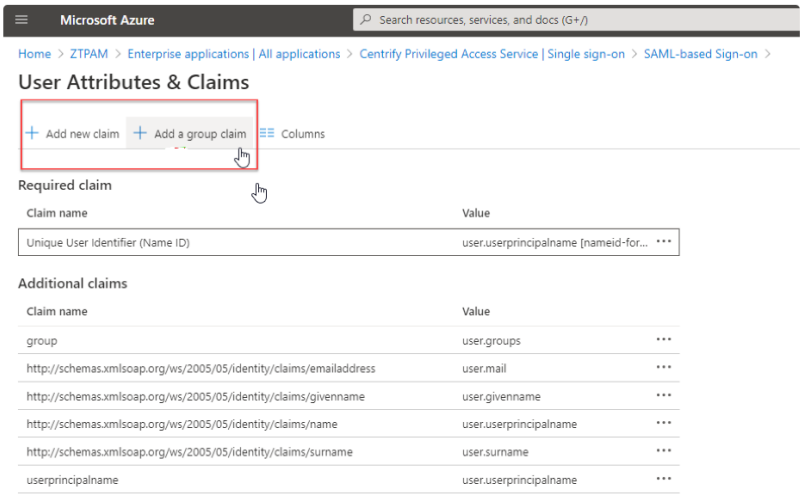
11. In the SAML Signing Certificate section, copy the value for App Federation Metadata Url.



12. In the Partner Management window, Inbound Metadata tab, under the field for Option 1: Upload configuration from URL paste the value you copied above and click **Save**.

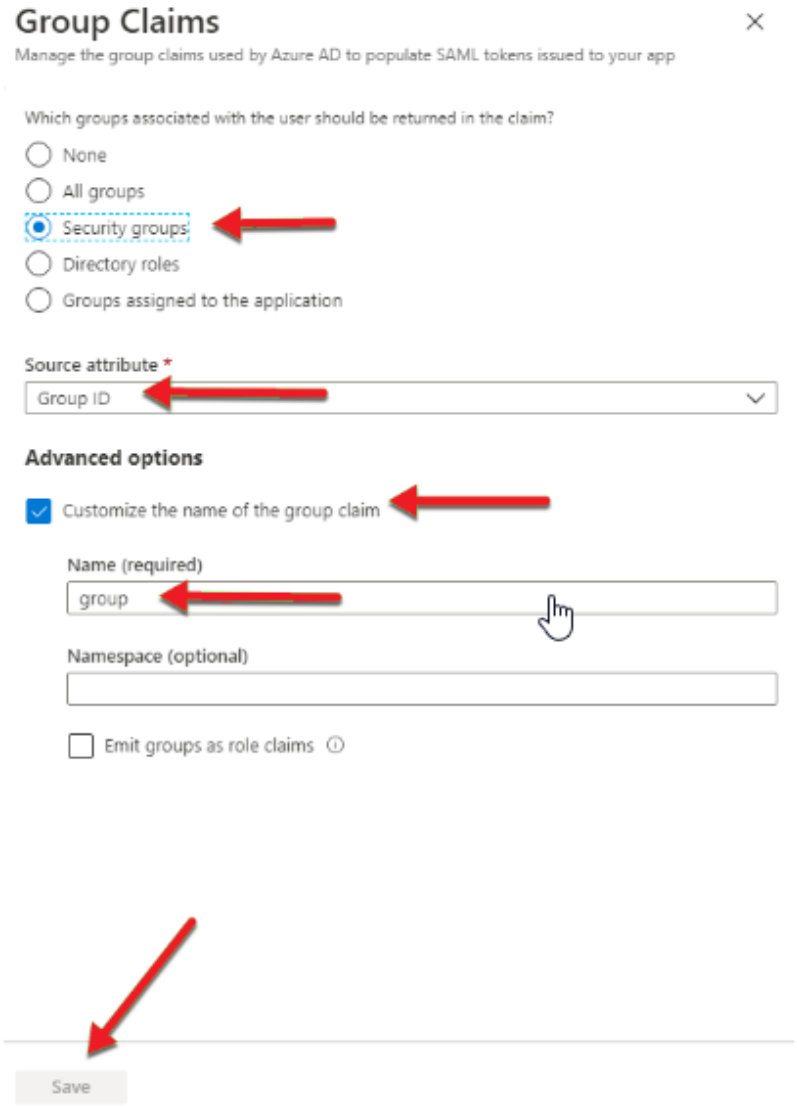


13. Automatically fill the username in Access Directory when performing an SP-initiated log on from Delinea PAS (to avoid having to type the usernametwice: once in Delinea PAS and once in Entra ID Integration). In the PartnerManagement window, at the **Inbound Metadata** tab, in the field for**Identity Provider Login URL** append /?login_hint=[username] to the URL value the and click **Save**.
14. Navigate back to Entra ID Integration, under the SAML configuration for the Delinea application and **Add a new claim**:



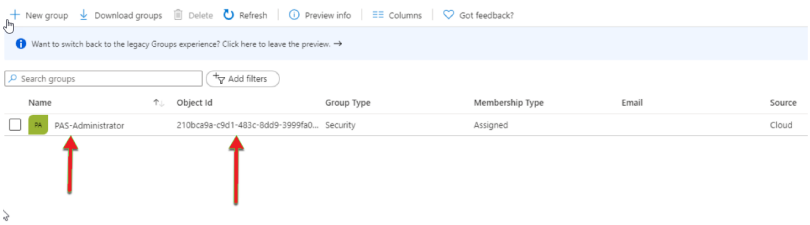
- **Name**: userprincipalname.
- **Source** Attribute: user.userprincipalname and **Add a group claim**:

The group claim name must contain the word "group":

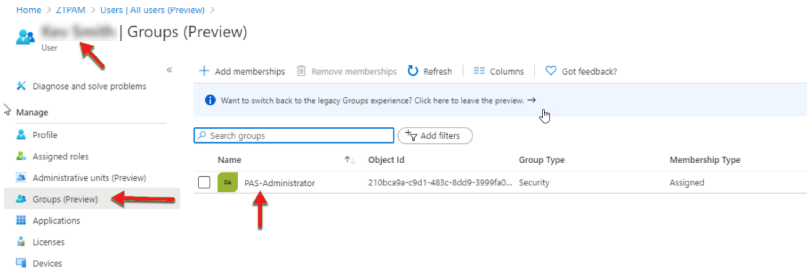


Lastly, save the configuration.

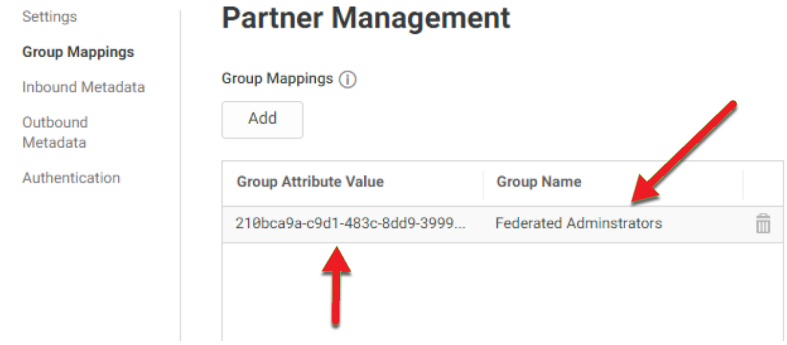
15. Create a new Entra ID group and note the **ObjectId**:



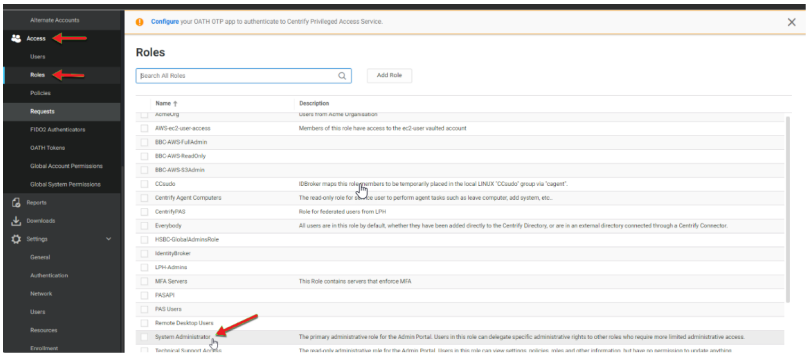
Ensure you are a member of this new Entra ID group:



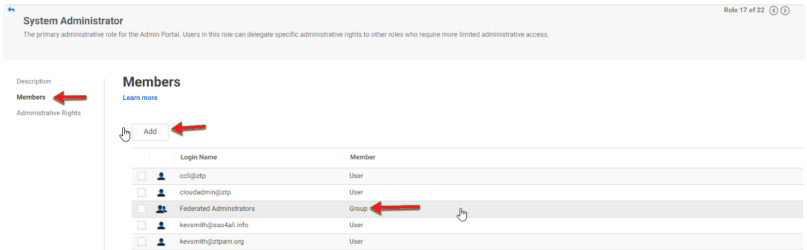
16. Navigate back to the Delinea PAS tenant. Navigate to **Partner Management** and add the group mapping using the **ObjectId** as the Group Attribute Value and a Group Name of your choice:



17. In Delinea PAS, add the Group Name to **System Administrator**. Navigate to **Access** > **Roles** and choose system administrator:



Click **Members** and add the group name you just added:



18. Save the configuration.

Testing the Microsoft Azure Active Directory Integration

To test the federation, you can do one of the following:

- From the Microsoft Azure Active Directory single sign-on overview page, select **Test this application** and follow the test steps.

- Log into Privileged Access Service using the Azure Active Directory domain account name you set up.

Integration with Okta

To integrate Delinea Privileged Access Service and Okta, review and perform the steps in the following sections:

- "Integration Prerequisites" below
- "Setting Up Security Assertion Markup Language (SAML)" below
- "Authenticating SAML" on page 1112
- "Testing Delinea PAS and Okta Federation" on page 1113

Integration Prerequisites

Before you begin the Delinea Privileged Access Service and Okta integration, ensure you have the following prepared in advance:

1. An Okta account with permission to create SAML applications.
2. A Delinea PAS account with administrative permission (to create a partner).

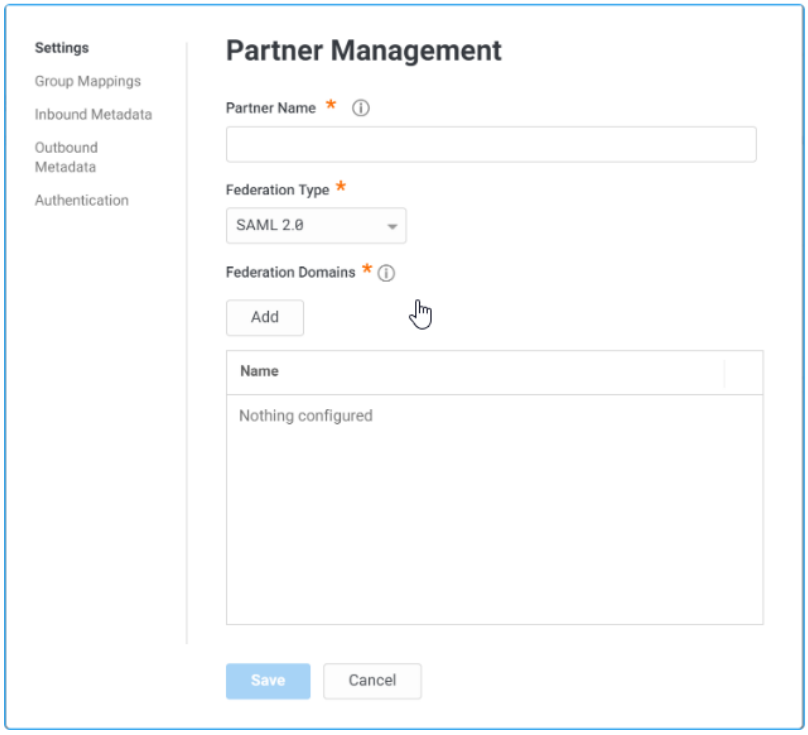
[title]: # (Setting up Security Assertion Markup Language (SAML)) [tags]: # (integrations,Okta) [priority]: # (32)

Setting Up Security Assertion Markup Language (SAML)

Configuring Delinea Privileged Access Service SAML

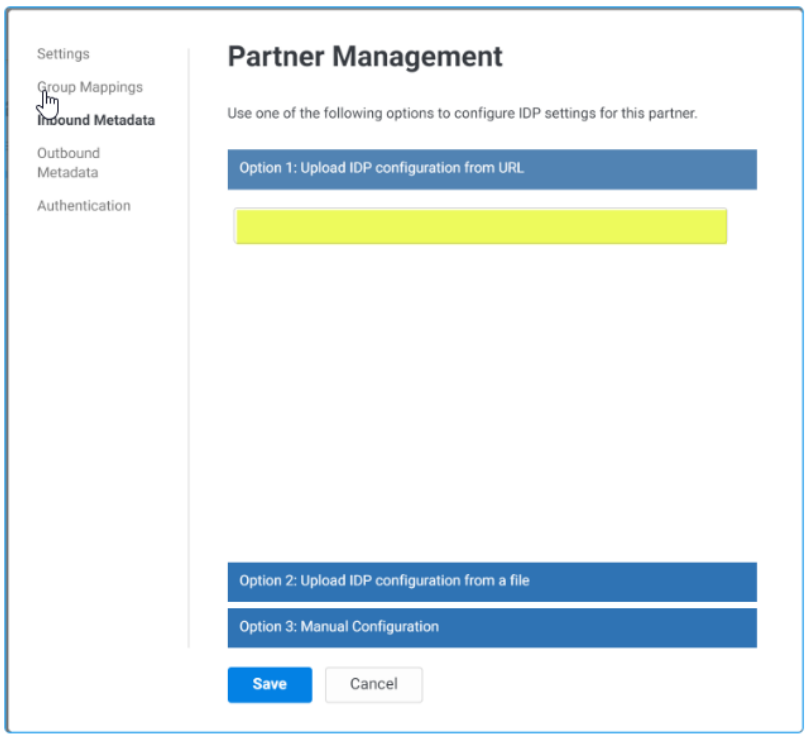
To configure Delinea for SAML, perform the following steps:

1. Open a browser tab or window to a Delinea PAS and navigate to **Settings** > **Users** > **Partner Management** and click **Add**.
2. On the main **Settings** tab, enter values in the following fields:

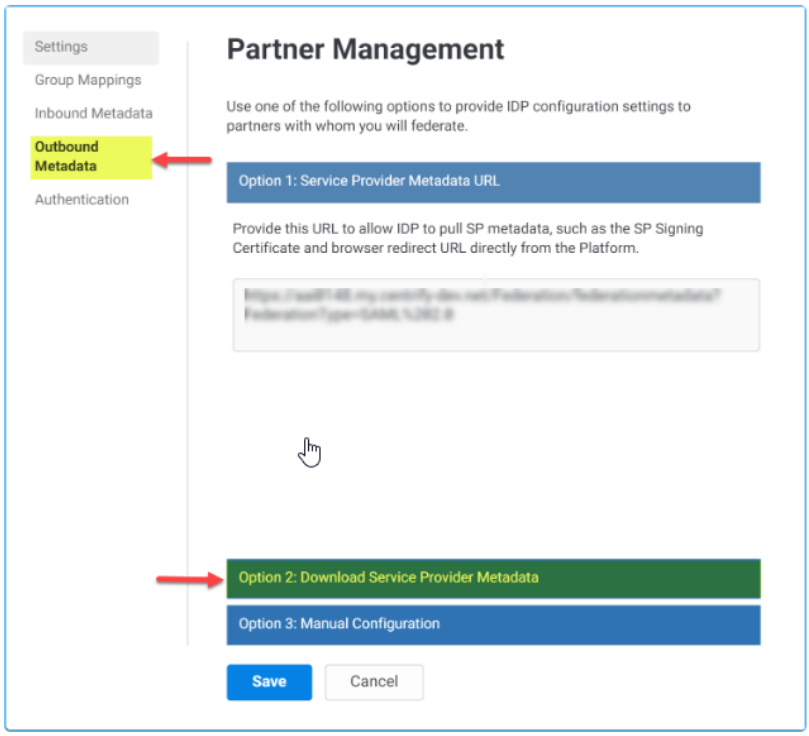


- **Partner Name** Okta.
- **Federation Type** SAML 2.0.
- Under **Federation Domains**, click **Add**, enter the domain for users and click **Add** again.

3. Select **Inbound Metadata**, provide a dummy IDP for now and do not save.



4. Select the **Outbound Metadata** tab and choose **Option 2: Download Service Provider Metadata**.



5. Click __Download Metadata__and open the downloaded XML file in a text editor.

Note: This file will be used below, when you configure Okta SAML.

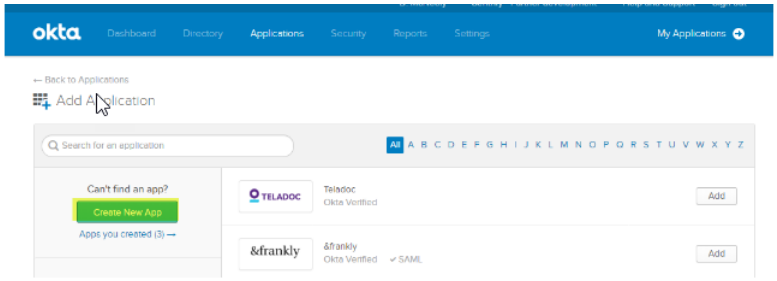
- Search for the XML tag **EntityDescriptor** and note the value of the **entityID** parameter.
- Search for the XML tag **AssertionConsumerService**, and note the value of the **Location** parameter.

Note: Do not click **Save**, continue with remaining configuration steps as detailed below.

Configuring Okta SAML

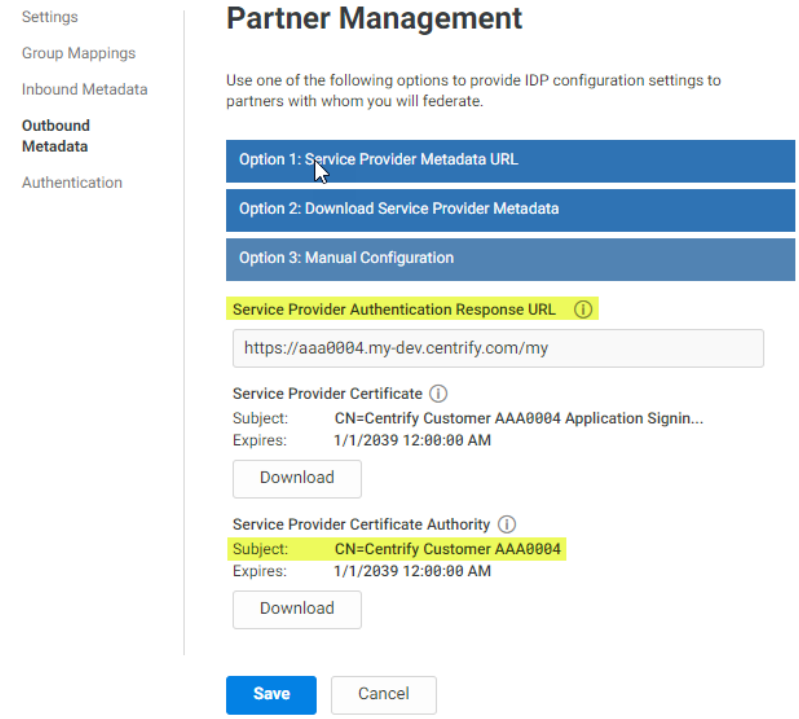
To configure Okta SAML, perform the following steps:

1. Open a new browser tab or window and navigate to the Okta dashboard. Navigate to **Directory** > **Groups**.
2. Add groups to use for granting rights within Delinea PAS.
3. Select the **Applications** tab, click **Add Application** and click **Create New App**, as seen below.



- Choose **Web** application, select **SAML 2.0**, and click **Create**.
- Enter the App name **Centrify Privilege Access Service**.
- Upload the Delinea logo.

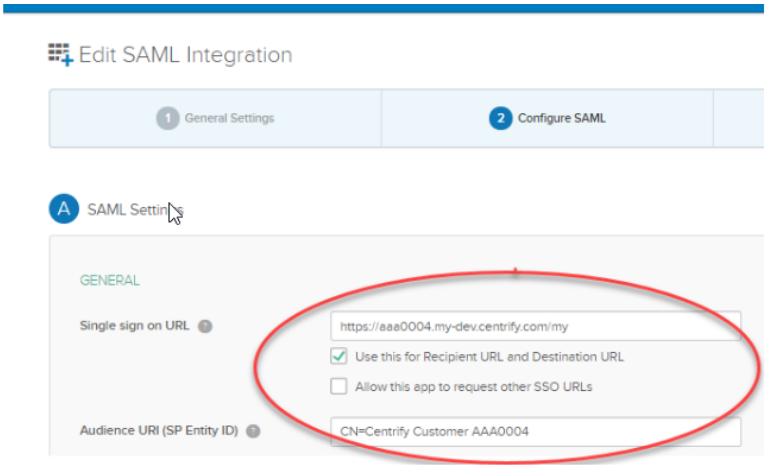
4. Going back to the Delinea PAS instance, copy the highlighed values:



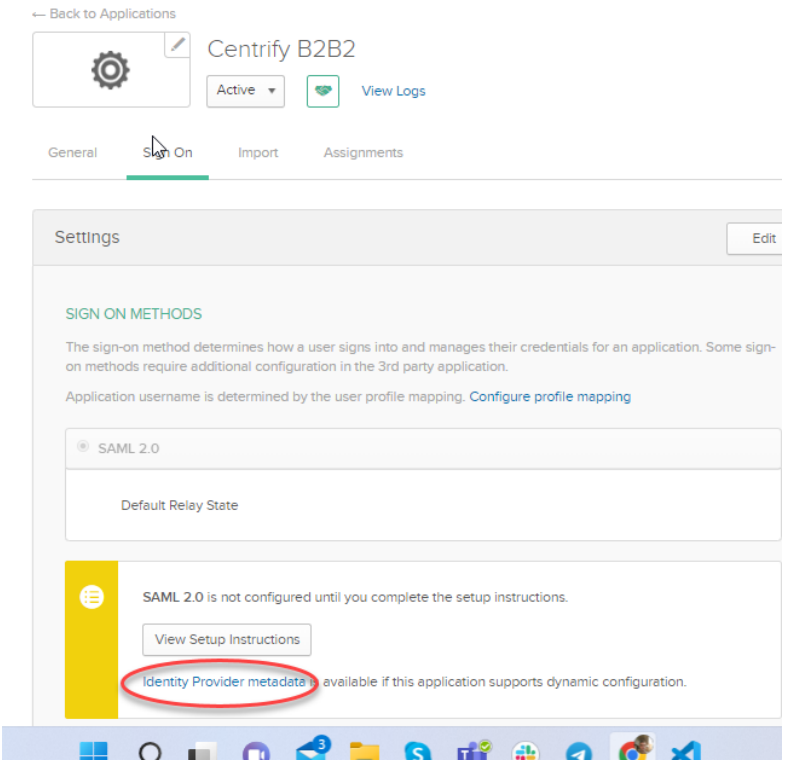
5. Click **Save**.

- Enter the Single sign on URL as the Delinea PAS tenant URL. For example, https://<tenantid>.my.centrify.net/home.
- Check the box for "Use this for Recipient URL and Destination URL."

Note: Do not check the box for "Allow this app to request other SSO URLs."

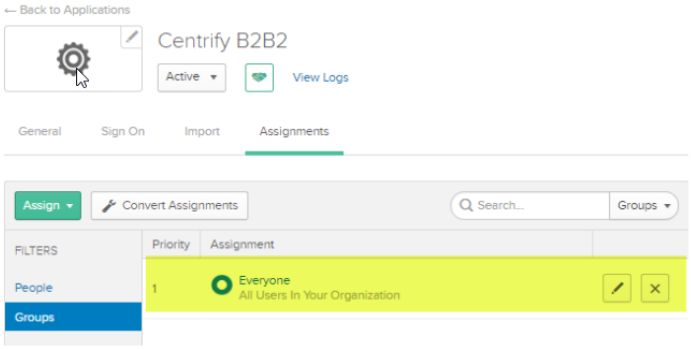


6. Using the entityID value from the downloaded XML file, enter **Audience URI**. For example, CN=Centrify:Customer:<tenant_id>.
7. Click **Show Advanced Settings**.
   - Change Honor Force Authentication to **Yes**.
   - In the Attribute Statements section, enter the following name-value pair:
   - Name=UserPrincipalName
   - Value set to user.email.
   - In the Group Attribute Statement section, enter the following name-value pair:
   - Name=Group
   - Filter Starts With Delinea or name of Groups created in the first step
8. Click **Next**. Select the desired options for the support questions. Click **Finish**.
9. Select the Delinea application, then select the **Sign On** tab.
10. Click the **Edit** button. Set the **Application username format** to **Email**.
11. Click the **Save** button.
12. Right-click **Identity Provider metadata** link and save the XML file containing the Okta certificate.



13. Click the **Assignments** tab.

14. Grant user and group rights to access/use the Delinea PAS application.



15. Make sure the users are also a member of one of the Okta Groups for permissions within Centrify PAS.

Confirming Delinea SAML Configuration

To confirm Delinea SAML configuration, perform the following steps:

1. Return to the Delinea PAS tenant browser, where you left off with "Setting Up Security Assertion Markup Language (SAML)" on page 1106.
2. Select **Inbound Metadata** tab, click **Option 2: Upload IDP Configuration from a file**. Select the Okta certificate file downloaded above and click **Save**.
3. Upload the XML file containing the Okta certificate.
4. Select the **Group Mappings** tab.
5. Map the Okta group names to a group name for the IDP.
6. Click **Save**.

Authenticating SAML

If you have Okta configured to use AD as the source directory whereby Privileged Access Service can see the same directory through the connector, choose from the following:

- Set up groups in Okta, add AD groups as members, and set up group mapping in the SAML partnership.
- Do not create groups in Okta, but configure Delinea PAS to look up the user in AD/LDAP and then use the directory groups for permission/rights within Delinea PAS. Instead, try one of the following:
- Force the lookup. If the user is not found, reject the login.
- Try the the lookup and use the groups (if present), but do not reject the login.
- Add groups from Okta into roles to grant permissions/rights within Delinea PAS.

Note: To customize the login session timeout value for user accounts federated from Okta to Delinea PAS, contact Delinea Support. This value is the duration for the user's login session. A suggested timeout value might be 4 hours, 8 hours, etc.

Testing Delinea PAS and Okta Federation

Identity Provider to Service Provider Authentication Confirmation

To confirm authentication between identity provider to service provider, perform the following steps:

1. Log into the Okta portal and click on the Delinea icon.
2. Verify that you are redirected to the Delinea PAS tenant dashboard.

Service Provider to Identity Provider Authentication Confirmation

To confirm service provider to identity provider authentication, perform the following steps:

Note: Ensure you are logged out of the Okta and Delinea PAS tenants.

1. Log into Delinea PAS with the domain given in partner federation and verify that you are redirected to the Okta login page.
2. Log into the Okta portal and verify that you are redirected to the Delinea PAS dashboard.

Okta Multi-Factor Authentication (MFA) Setup

To set up Okta MFA, perform the following steps:

1. Log in as the administrator to the Okta portal. At the top left, select **Classic UI**.
2. Select the **Applications** tab.
3. Click **Add Application**.
4. Search for **RADIUS Application** and click **Add**.
5. Enter **Delinea RADIUS MFA** for the Application label, click **Next**.
6. Check **Okta performs primary authentication**. (This configuration works for versions 19.4 and below when Delinea PAS is not federated to thedomain. Version 19.5 and above can be federated to the domain and use Okta as the master authenticator.)
7. For **UDP Port** enter 1812.
8. For **Secret Key** enter a secret key (will be entered into Delinea PAS also).
9. For **Application username format** select Email.
10. For **Update application username on** select Create and Update.
11. Click **Done**.
12. Install the Okta RADIUS Agent on an accessible host (for example, an active connector host). For instructions on how to install the agent, see the Oktadocumentation: https://help.okta.com/en/prod/Content/Topics/Directory/Agent_Installing_the_Okta_Radius_Agent.htm.

Delinea Privileged Access Service Setup

To set up Delinea PAS, perform the following steps:

1. Log into the Delinea PAS console as administrator.
2. Navigate to **Settings** > **Network** > **Delinea Connectors**. Select an active Connector. Select the **RADIUS** tab. Check the box "Enable connections to external RADIUS servers." Click **Save**.
3. Navigate to **Settings** > **Authentication**. Select the **RADIUS Connections** tab, select **Servers**, and click **Add**.
4. Set **Name** to Okta, enter the hostname or IP address of the host where the Okta RADIUS Agent was installed.

- Set **Port** to 1812.
- set the **Server Secret** to the same value entered into the Okta portal.
- Set the **Receive Timeout** to 30.
- set **User Identifier Attribute** to Email.
- set **Response Input Label** to Password.
- Click **Save**.

5. Navigate to **Settings** > **Authentication** > **Authentication Profiles** and click **Add Profile**.

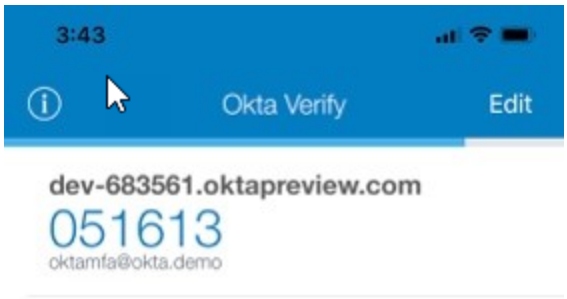
- For **Profile Name** enter Okta MFA Authentication Profile.
- For Challenge 1 check third Party RADIUS Authentication.
- Do not check any other authentication mechanisms.
- Click **OK**.

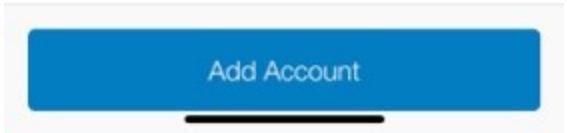
6. Navigate to **Access** > **Roles** and create Role Okta MFA User. Set administrative rights to allow Admin Portal Login at a minimum. Add one ormore users as members of the role (in this example: oktamfa@okta.demo). Click **Save**.
7. Navigate to **Access** > **Policies** and click **Add Policy Set**.
8. Enter the name Okta MFA Policy for the policy, and for Policy Assignment select Specified Roles.
9. Click **Add** and select a role containing the Okta MFA users (in this example: Okta MFA User).
10. Navigate to **Authentication Policies** > **Delinea Services**. Set **Enable authentication policy controls** to Yes and set the **Default Profile** to Okta MFA Authentication Profile.
11. Under **User Security Policies** > **RADIUS**, set **Allow Third Party RADIUS Authentication** to Yes.
12. Save the policy.

Testing Okta MFA

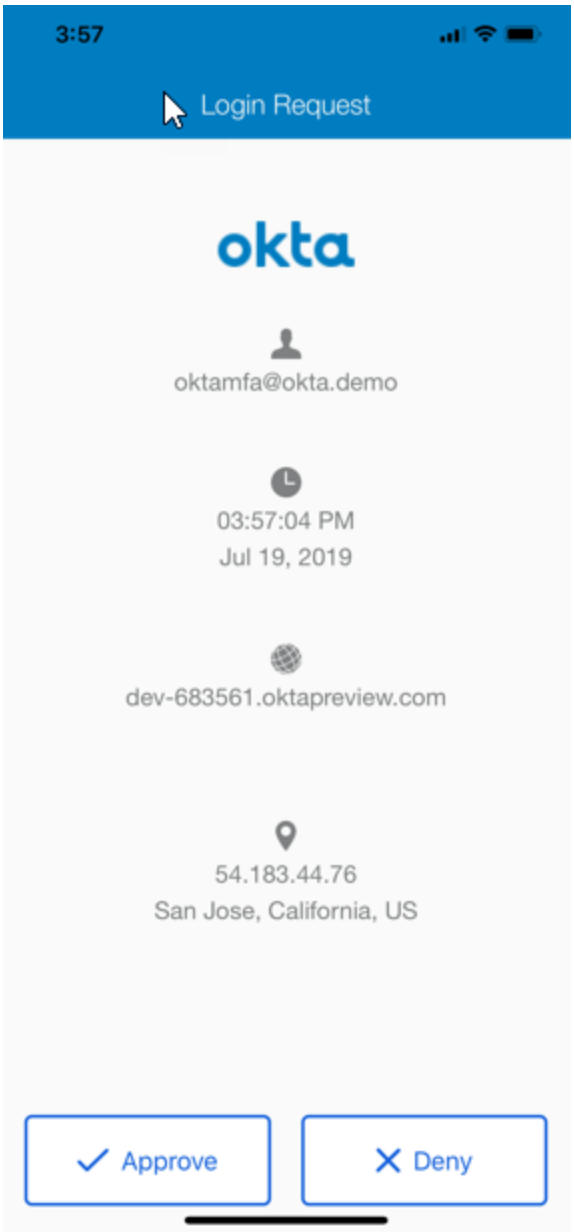
To test Okta MFA, perform the following steps:

1. Verify that the Okta username is enrolled in your Okta MFA mobile application.
2. Open an incognito browser window and go to the Admin Portal.
3. Enter the PIN from the Okta application or enter 1 and approve the request in the Okta application.





4. On successful MFA, the user will be logged into the Delinea PAS portal.



Integrating with PingOne Enterprise

Integration prerequisites

- Delinea PAS tenant.
- PingOne for Enterprise tenant.

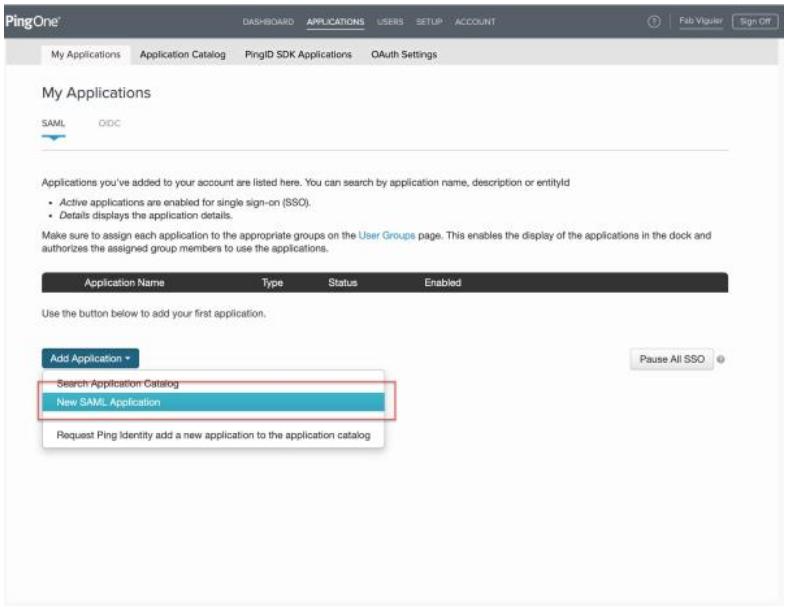
Configuring SAML Single Sign-On (SSO) for PingOne Enterprise

The following steps detail how to set up PingOne for Enterprise as an Identity Provider (IdP). In this configuration, Delinea PAS is the Service Provider (SP). Once configured you can access Delinea PAS from PingOne for

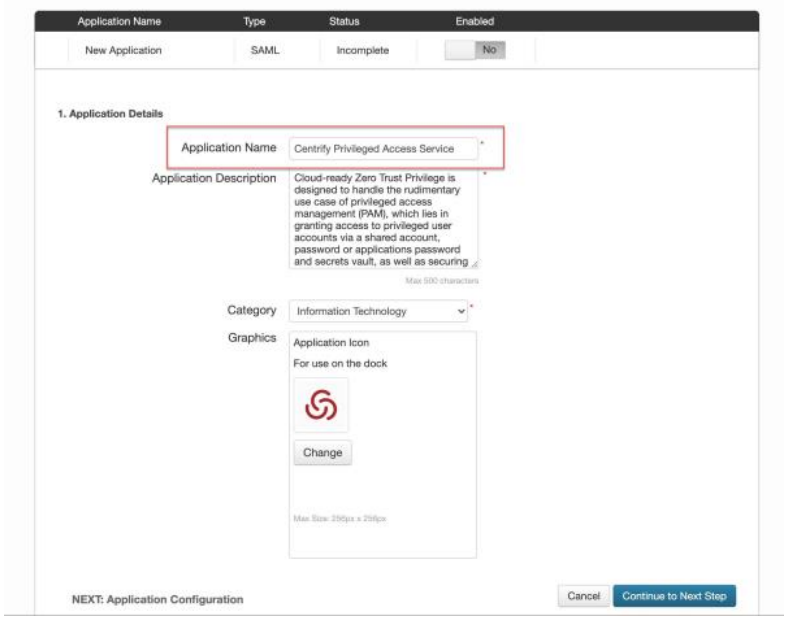
Enterprise using SAML Single Sign-On (SSO).

To configure the PingOne tenant for SSO

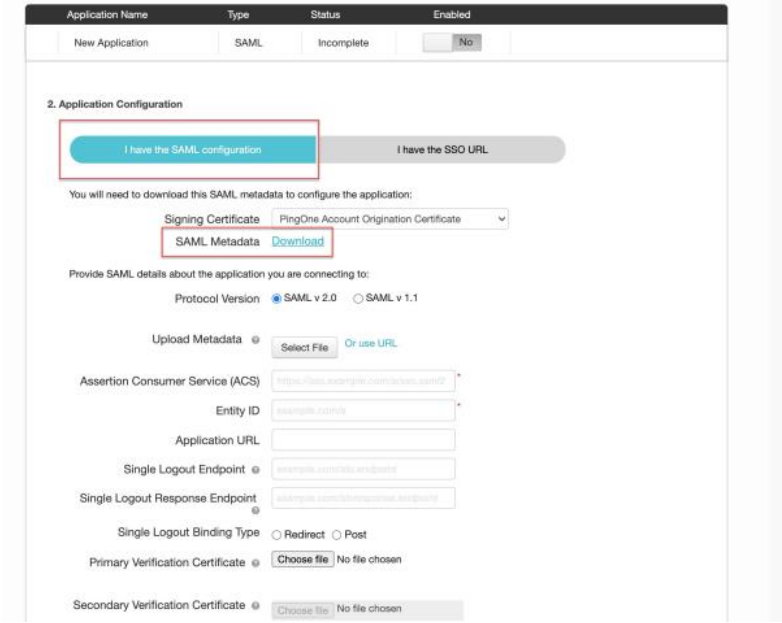
1. In the PingOne tenant, navigate to **Applications** > **Add Application** > **New SAML Application**.



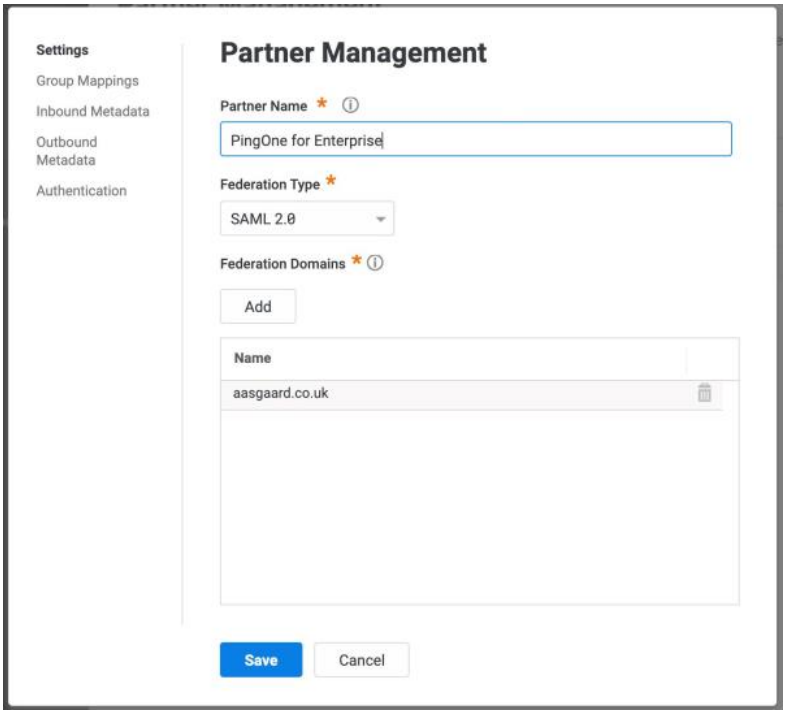
Name the Application Delinea Privileged Access Service" and (optionally) add description. upload logo, then click **Continue to Next Step**.



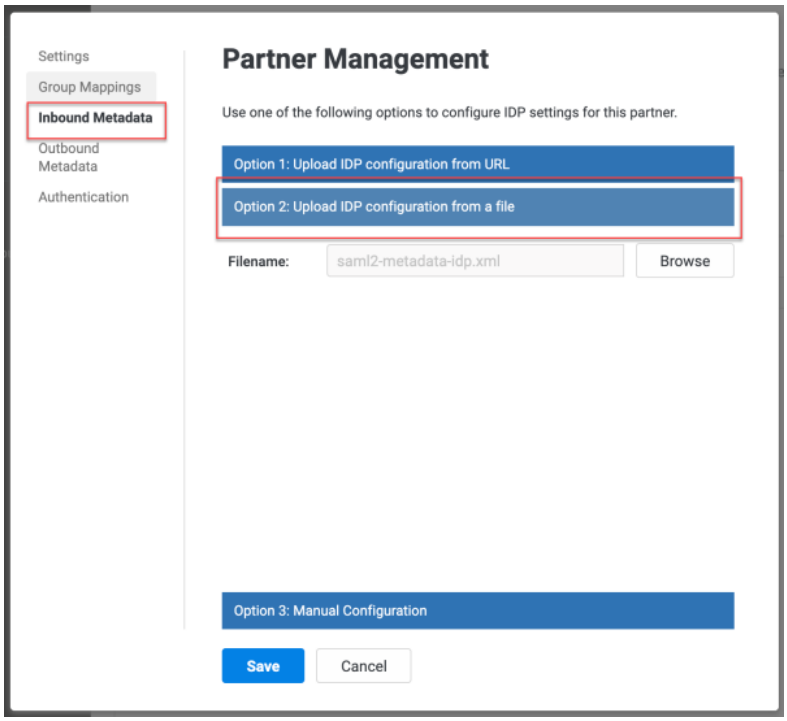
2. Choose **I have the SAML Configuration**, then click the **SAML Metadata** download link (this saves an XML file named "saml2-metadata-idp.xml").



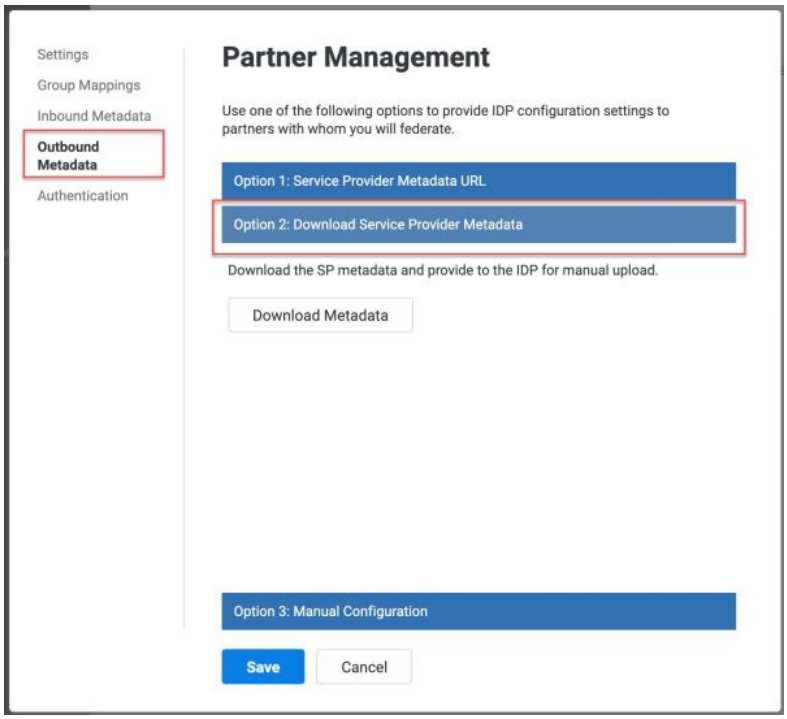
3. Navigate to the Delinea PAS tenant. In the Delinea PAS tenant. Navigate to **Settings** > **Users** > **Partner Management** then click **Add**.
4. Under **Settings**, name the Partner configuration “PingOne for Enterprise”, choose SAML 2.0 as a federation type and add the domain name(s) that can be used as suffix for SP-initiated login by users (will depend on your environment and authentication methods)



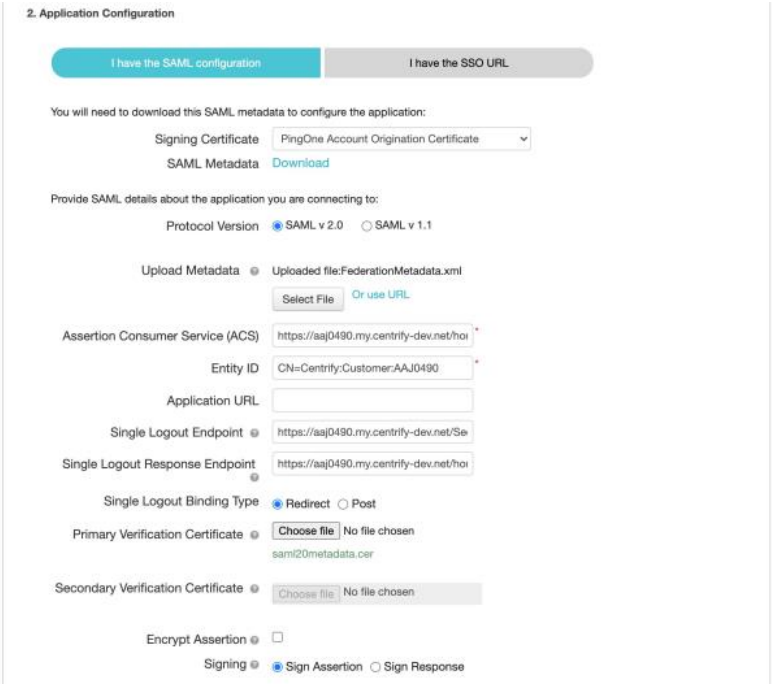
5. Under **Inbound Metadata**, choose Option 2 and upload the XML file obtained from PingOne.



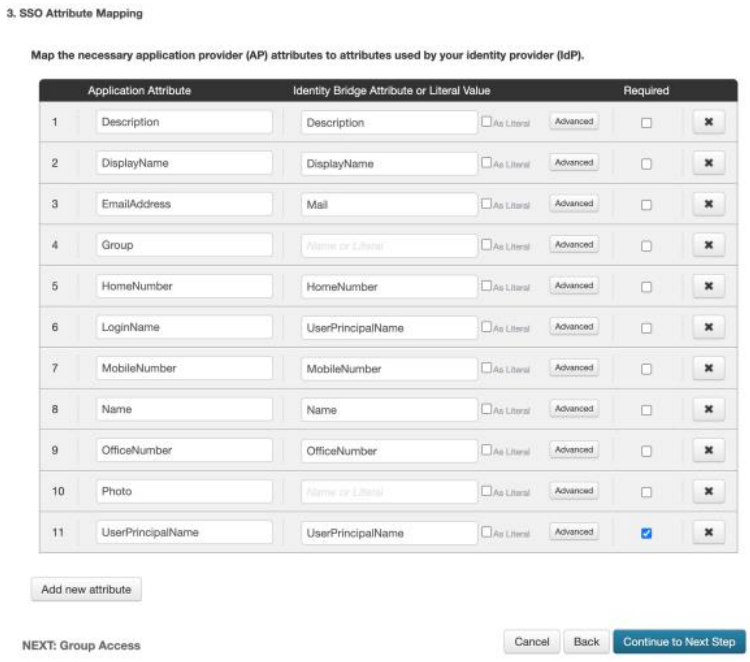
Under **Outbond Metadata** section, choose Option 2 and then Download the metadata file (this saves an XML file named “”).



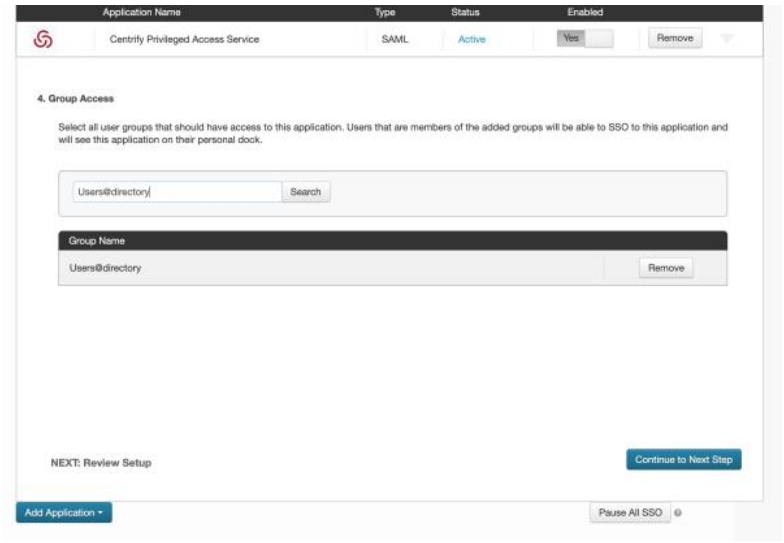
6. Save the configuration.
7. Go back to the PingOne application configuration. On the PingOne tenant, continue the application configuration under the **I Have the SAML Configuration** section.
8. Upload the metadata file you obtained from the Delinea Partner configuration and **Continue to Next Step**.



9. Configure attribute mapping. This configuration may differ based on the directory used to login. In the example below, both PingOne and Delinea PAS are configured to authenticate Active Directory users from the same domain and therefore most attributes will match literally. You may need to change attribute name or use advanced mapping to adapt to your environment. Once you have concluded mapping, click **Continue to Next Step**.



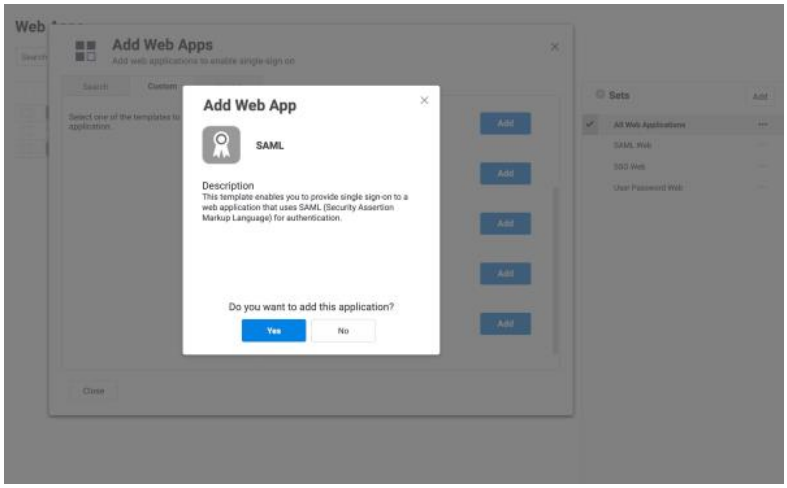
10. Add group(s) that will be allowed to use the application (example: Users@directory is everyone on the Ping Directory) and click **Continue to Next Step**.



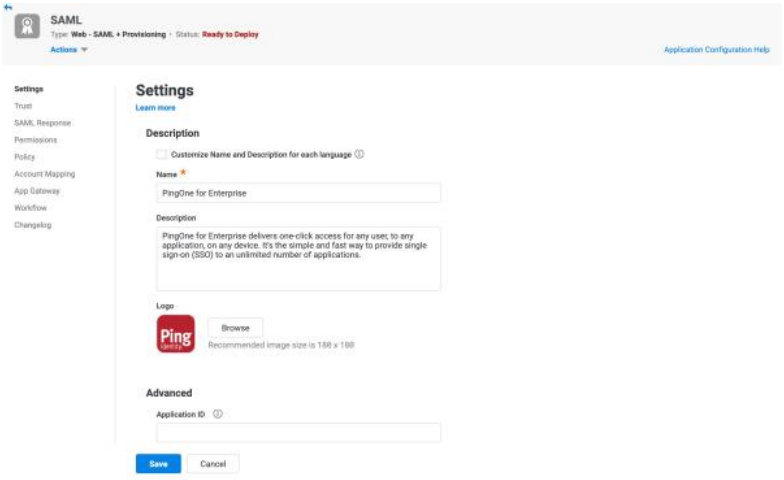
11. Review and click **Finish**.

Configuring Delinea PAS as an Identity Provider

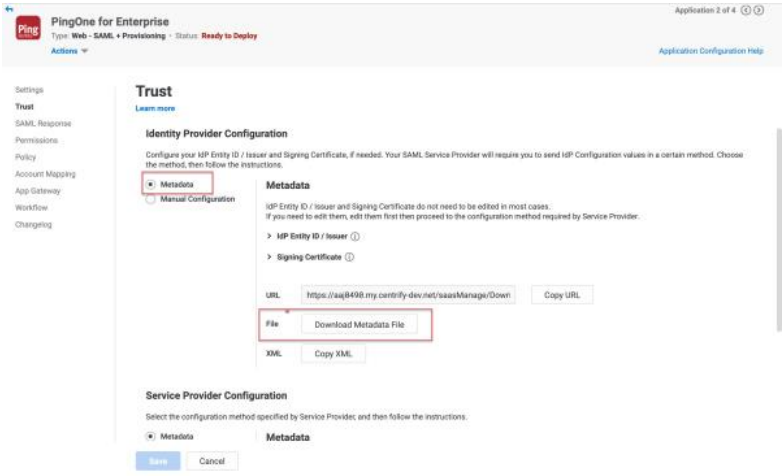
1. In the Delinea PAS tenant, navigate to **Apps** > **Web Apps** and click **Add Web Apps**.
2. On the **Custom** tab, choose **SAML** template and click **Add** and confirm **Yes**.



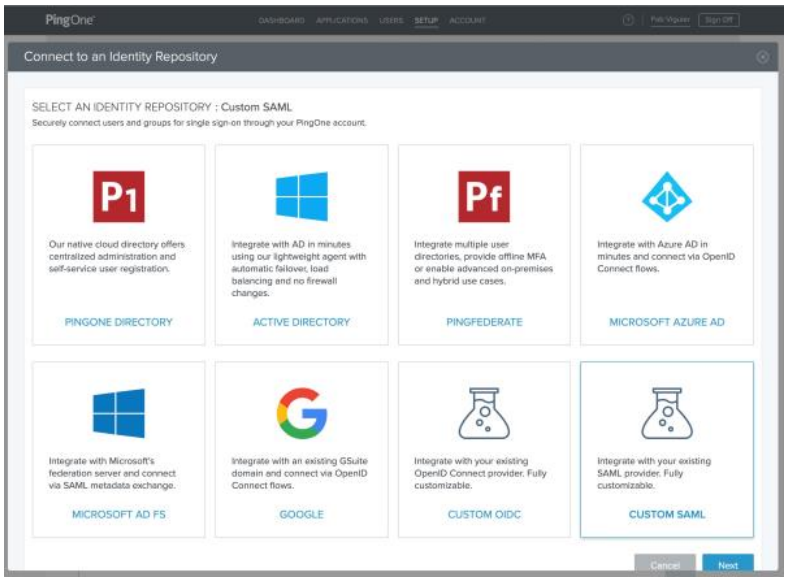
3. Under **Settings** tab, name the App “PingOne for Enterprise” and (optionally) add description and upload logo.



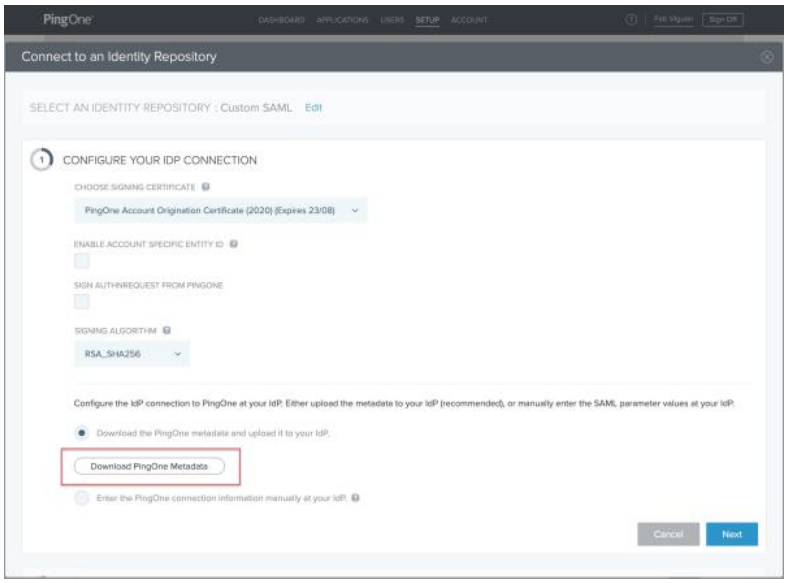
4. Under the **Trust** tab and in the **Identity Provider Configuration** section, choose **Metadata** and click **Download Metadata File** (will saves an XML file named “PingOne for Enterprise - IdP Metadata.xml”).



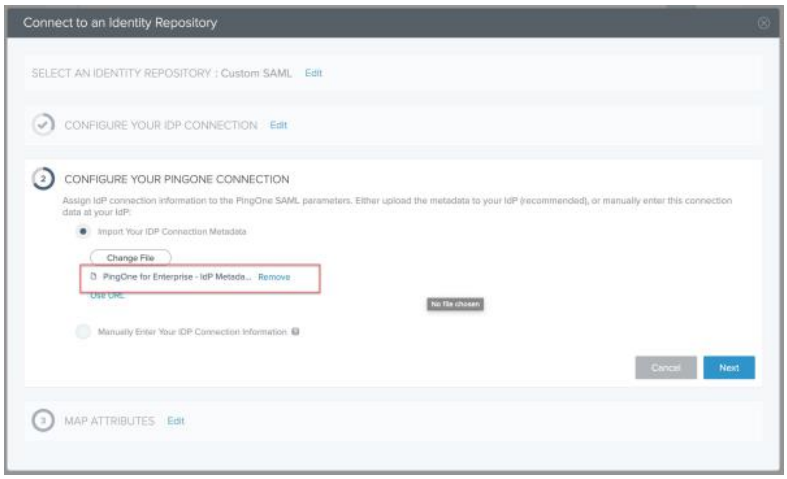
5. Click **Save**.
6. Navigate back to the PingOne tenant. In the PingOne tenant, navigate to **Setup** and either **Add a new Identity Repository** or change the existing one.
7. Select **Custom SAML** as the Identity Repository type and click **Next**.



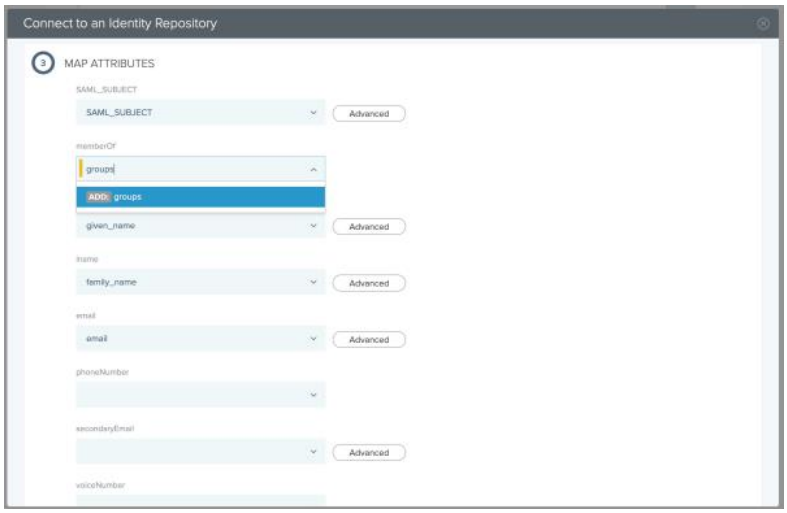
8. Under **Configure Your IDP Connection**, click **Download PingOne Metadata** then **Next** (this saves an XML file named “pingone-metadata.xml”).



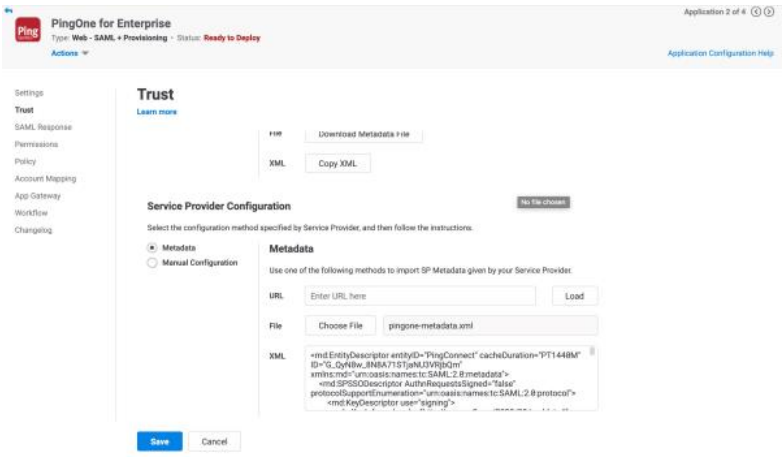
9. Under **Configure Your PingOne Connection** , import the IdP Metadata file named “PingOne for Enterprise - IdP Metadata.xml” and click **Next**.



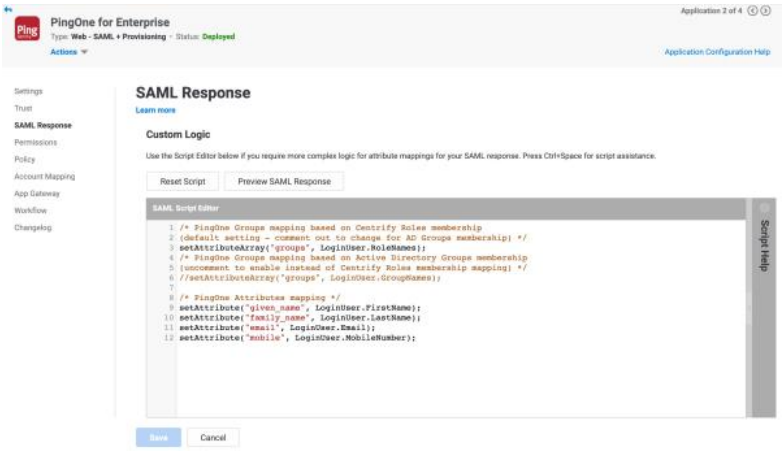
10. Under the **Map Attributes** section, add a variable named “groups”. You can add other mapping attributes based on your configuration needs.



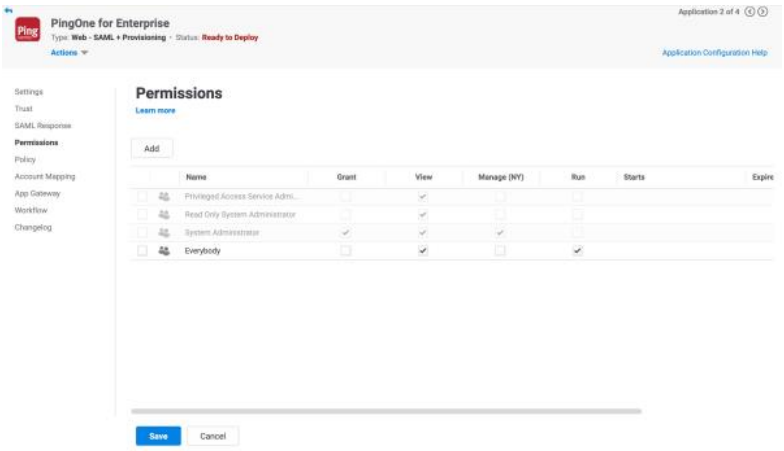
11. Click **Save**.
12. Navigate back to the Delinea PAS tenant. In the Delinea PAS tenant, navigate to **Apps** > **Web Apps** and edit the “PingOne for Enterprise” application setting.
13. Under **Trust** and in the **Service Provider Configuration** section, choose **Metadata** and click **Choose File**, upload the file named “pingone-metadata.xml”.



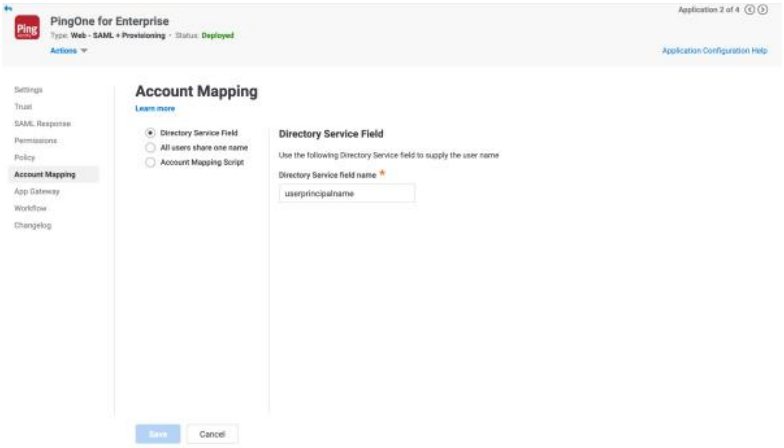
14. Under **SAML Response**, and the **Custom Logic** section, edit the SAML script. The sample below is provided as an example, you may want to add other attributes if you modified the Map Attributes list under PingOne configuration.



15. Under **Permissions**, add the list of wsers and/or roles that have permissions to launch the application (use of a role should be always preferred for ease of access management).



16. Under **Account Mapping**, choose how the user will be recognized under PingOne for Enterprise. The default to UserPrincipalName when using Active Directory could be using email or any other value that suits your environment (this value should be unique).



Integration With Tenable IO

The following documents how to integrate Tenable applications with Privileged Access Service. For the latest on integrating with Tenable IO, see the Tenable documentation.

Before You Begin

To properly integrate Tenable with Delinea PAS you must meet the following requirements:

- You must have an active account for at least one of the following Tenable products to integrate with Delinea: Tenable.io or Nessus Manager.
- Tenable User Role. You must have the appropriate role for your Tenable account as listed below:
- Tenable.io - Standard, Scan Manager, Administrator, or System Administrator

- Nessus Manager - Standard, Administrator, or System Administrator.
- You must have an active Delinea PAS account.

Configuring Nessus for PAS

To configure Nessus for Delinea PAS, perform the following steps:

- "To Configure the Nessus Manager with Privileged Access Service for Windows" below
- "Configuring Nessus for PAS" above

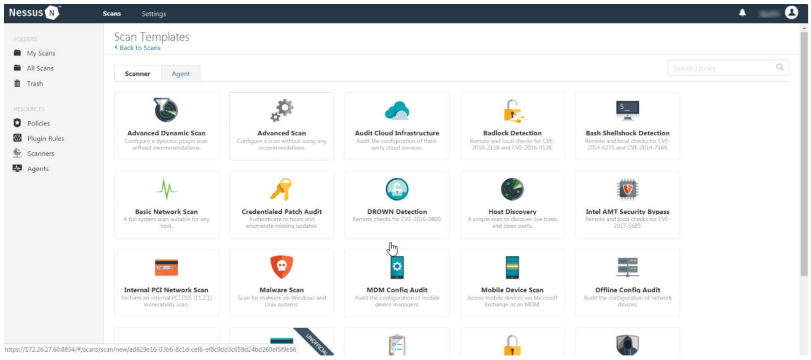
Requirements

- Nessus Manager account.
- Delinea Privileged Access Service account.
- Required User Role: Standard, Administrator, or System Administrator.

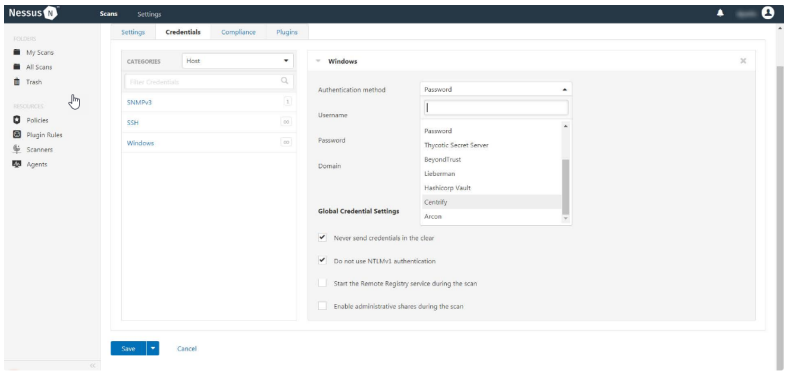
To Configure the Nessus Manager with Privileged Access Service for Windows

To configure Nessus Manager with Delinea PAS using Windows credentials, complete the following steps:

1. Log into Nessus Manager. Click **Scans**. The **My Scans** page appears.
2. Click **New Scan**. The **Scan Templates** page appears:



3. Select a scan template. The selected scan template **Settings** page appears.
4. In the **Name** field, enter a name for the scan.
5. In the **Targets** field, enter an IP address, hostname, or range of IP addresses.
6. (Optional) Add a description, folder location, scanner location, and specify target groups.
7. Click the **Credentials** tab. The Credentials options appear. By default, the **Categories** drop-down box displays Host.
8. In the left menu, select **Windows**. The Windows settings appear.
9. In the **Windows** settings, click the **Authentication method** drop-down box. The Authentication method drop-down box options appear.



10. Select **Delinea**. The Delinea options appear.
11. Configure the Windows credentials.

Option	Default Value
Centrify Host	(Required) The Centrify IP address or DNS address. **Note:** If your Centrify installation is in a subdirectory, you must include the subdirectory path. For example, type IP address or hostname/sub- directory path.
Centrify Port	The port on which Centrify listens.
API User	(Required) The API user provided by Centrify
API Key	(Required) The API key provided by Centrify.
Tenant	The name of a specified team in a multi-team environment.
Authentication URL	The URL Nessus Manager uses to access Centrify.
Password Engine URL	The name of a specified team in a multi-team environment.
Username	(Required) The username to log in to the hosts you want to scan.

Option	Default Value
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in Centrify. Configure the Checkout Duration to exceed the typical duration of your Nessus Manager scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note**: Configure the password change interval in Centrify so that password changes do not disrupt your Nessus Manager scans. If Centrify changes a password during a scan, the scan fails.
Use SSL	If enabled, Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.
Verify SSL	If enabled, Nessus Manager validates the SSL certificate. You must con- figure SSL through IIS in Centrify before enabling this option.

12. Click **Save**. The credential saves and the **My Scans** page appears.

    To verify the integration is working:

13. On the **My Scans** page, click **Launch** to initiate an on-demand scan.
14. Once the scan completes, select the completed scan and look for the following message - Microsoft Windows SMB Log In Possible: 10394. This result validates that authentication was successful.

Configuring Nessus for Delinea PAS (SSH)

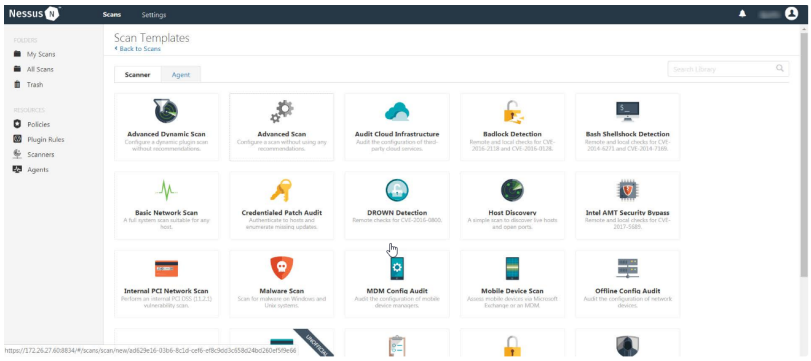
Perform the following steps to configure Nessus with Delinea PAS using SSH.

Requirements

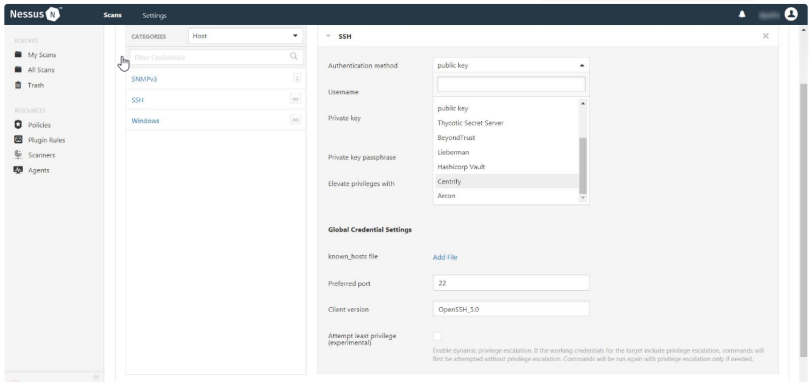
- Nessus Manager account.
- Delinea PAS account.
- Required User Role: Standard, Administrator, or System administrator.

To integrate Nessus with Privileged Access Service using SSH credentials:

1. Log into Nessus Manager. Click **Scans**. The **MyScans** page appears.
2. Click **+ New Scan**. The **Scan Templates** page appears:



3. Select a scan template. The selected scan template Settings page appears.
4. In the **Name** field, type a name for the scan.
5. In the **Targets** field, type an IP address, hostname, or range of IP addresses.
6. (Optional) Add a description, folder location, scanner location, and specify target groups.
7. Click the **Credentials** tab. The Credentials options appear. By default, the Categories drop-down box displays Host.
8. In the left menu, select **SSH**. The SSH settings appear.
9. In the SSH settings, click the **Authentication** method drop-down box. The Authentication method drop-down box options appear.



10. Select **Delinea**. The Delinea options appear.
11. Configure the SSH credentials.

Option	Default Value
Centrify Host	(Required) The Centrify IP address or DNS address. **Note**: If your Centrify installation is in a subdirectory, you must include the subdirectory path. For example, type IP address or hostname/sub- directory path.

Option	Default Value
Centrify Port	The port on which #Centrify listens.
API User	(Required) The API user provided by Centrify
API Key	(Required) The API key provided by Centrify.
Tenant	The name of a specified team in a multi-team environment.
Authentication URL	The URL Nessus Manager uses to access Centrify.
Password Engine URL	The name of a specified team in a multi-team environment.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in Centrify. Configure the Checkout Duration to exceed the typical duration of your Nessus Manager scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note**: Configure the password change interval in Centrify so that password changes do not disrupt your Nessus Manager scans. If Centrify changes a password during a scan, the scan fails.
Use SSL	If enabled, Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.
Verify SSL	If enabled, Nessus Manager validates the SSL certificate. You must con- figure SSL through IIS in Centrify before enabling this option.

12. Click **Save**.

To verify the integration is working:

13. On the **My Scans** page, click **Launch** to initiate an on-demand scan.
14. Once the scan completes, select the completed scan and look for Plugin ID 97993 and the corresponding message - It was possible to log into the remotehost via SSH using 'password' authentication. This result validates that authentication was successful.

Configuring Tenable.io for Privileged Access Service

To configure Tenable.io for Delinea PAS, perform the following steps:

- "Configuring Tenable.io With Delinea PAS (Windows)" on the next page
- "Configuring Tenable.io for Privileged Access Service (SSH)" on page 1134

Configuring Tenable.io With Delinea PAS (Windows)

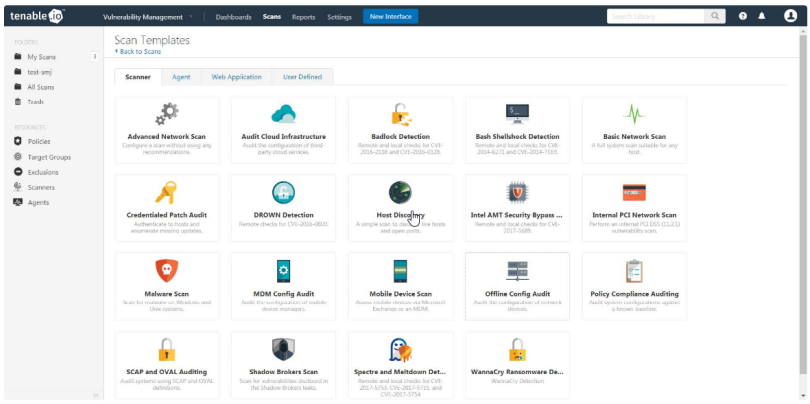
Complete the following steps to configure Tenable.io with Privileged Access Service using Windows.

Requirements

- Tenable.io account.
- Delinea PAS account.
- Required User Role: Standard, Scan Manager, or Administrator.

To integrate Tenable.io with Privileged Access Service using Windows credentials:

1. Log into Tenable.io. In the top navigation bar, click **Scans**. The **MyScans** page appears.
2. Click **+ New Scan**. The **Scan Templates** page appears.



3. Select a scan template. The selected scan template **Settings** page appears.
4. In the **Name** field, enter a name for the scan.
5. In the **Targets** field, enter an IP address, hostname, or range of IP addresses.
6. (Optional) Add a Description, Folder location, Scanner location, and specify Target groups.
7. Click the **Credentials** tab. The Credentials options appear.
8. In the left-hand menu, click the **Windows** option. The Credentials options appear. By default, the **Categories** drop-down box displays **Host**.
9. In the **Windows** section, click the **Authentication** method drop-down box. The **Authentication** method drop-down box options appear.
10. Select **Delinea**. The Delinea options appear.
11. Configure the Windows credentials.

Option	Default Value
Centrify Host	(Required) The Centrify IP address or DNS address. **Note**: If your Centrify installation is in a subdirectory, you must include the subdirectory path. For example, type IP address or hostname/sub- directory path.
Centrify Port	The port on which Centrify listens.
API User	(Required) The API user provided by Centrify
API Key	(Required) The API key provided by Centrify.
Tenant	The name of a specified team in a multi-team environment.
Authentication URL	The URL Tenable.io uses to access Centrify.
Password Engine URL	The name of a specified team in a multi-team environment.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in Centrify. Configure the Checkout Duration to exceed the typical duration of your Tenable.io scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note**: Configure the password change interval in Centrify so that password changes do not disrupt your Tenable.io scans. If Centrify changes a pass- word during a scan, the scan fails.
Use SSL	If enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.
Verify SSL	If enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.

12. Click **Save**. The credential saves and the **My Scans** page appears.

Verify the integration is working.

1. On the **My Scans** page, click **Launch** to initiate an on-demand scan.
2. Once the scan completes, click the completed scan. The scan details appear. Look for a message similar to the following- Microsoft Windows SMB Log In Possible: 10394. This validates that authentication was successful.

Configuring Tenable.io for Privileged Access Service (SSH)

Complete the following steps to configure Tenable.io with Delinea PAS using SSH.

Requirements

- Tenable.io account.
- Delinea PAS account.
- Required User Role: Standard, Scan Manager, or Administrator.

To configure Tenable.io for Delinea SSH:

1. Log in to Tenable.io. In the top navigation bar, click **Scans**. The **My Scans** page appears.
2. Click **+ New Scan**. The **Scan Templates** page appears.
3. Select a scan template. The selected scan template **Settings** page appears.
4. In the **Name** field, type a name for the scan.
5. In the **Targets** field, type an IP address, hostname, or range of IP addresses.
6. (Optional) Add a description, folder location, scanner location, and specify target groups.
7. Click the **Credentials** tab. The Credentials options appear.
8. In the left-hand menu, click the **SSH** option. The SSH section appears.
9. In the **Windows** section, click the **Authentication** method drop-down box. The **Authentication** method drop-down box options appear.
10. Select **Delinea**. The Delinea options appear.
11. Configure the SSH credentials.

Option	Default Value
Delinea Host	(Required) The Delinea IP address or DNS address. **Note**: If your Delinea installation is in a subdirectory, you must include the subdirectory path. For example, type IP address or hostname/sub- directory path.
Delinea Port	The port on which Delinea listens.
API User	(Required) The API user provided by Delinea
API Key	(Required) The API key provided by Delinea.
Tenant	The name of a specified team in a multi-team environment.
Authentication URL	The URL Tenable.io uses to access Delinea.
Password Engine URL	The name of a specified team in a multi-team environment.
Username	(Required) The username to log in to the hosts you want to scan.

Option	Default Value
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in Delinea. Configure the Checkout Duration to exceed the typical duration of your Tenable.io scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note**: Configure the password change interval in Delinea so that password changes do not disrupt your Tenable.io scans. If Delinea changes a pass- word during a scan, the scan fails.
Use SSL	If enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in Delinea before enabling this option.
Verify SSL	If enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in Delinea before enabling this option.

12. Click **Save**.

To verify the integration is working:

1. On the **My Scans** page, click **Launch** to initiate an on-demand scan.
2. Once the scan has completed, select the completed scan and look for Plugin ID 97993 and the corresponding message - It was possible to log into theremote host via SSH using 'password' authentication. This result validates that authentication was successful.

SIEM Integrations

Integration with ArcSight

This guide is written to assist Delinea customers with the task of easily integrating event data in ArcSight.

You can leverage the Delinea Add-on for ArcSight to normalize Delinea events in ArcSight so that you can view Centrify Server Suite events when you use the ArcSight Console. For example, a sample event payload for an event named, Run as role failure, looks like this:

```
Apr 19 17:19:46 member.centrify.vms dzagent[1404]: WARN AUDIT_TRAIL|Centrify
Suite|DirectAuthorize - Windows|1.0|18|Run as role failure|7|user=dwirth@centrify.vms
userSid=S-1-5-21-3883016548-1611565816-1967702834-1107 sessionId=3 centrifyEventID=6018
role=ROLE_SYSTEM_Archt/Global desktopguid=9766a262-c07b-4dbc-bad7-8a48d1fa3983
command=C:\\Program Files\\Centrify\\DirectManage Audit\\AuditManager\\Centrify
DirectManage Audit Manager.msc reason=The user name or password is incorrect
desktopname=Default networkroles=ROLE_SYSTEM_Archt/Global passwordprompted=True
```

This integration guide applies to the following ArcSight versions and Centrify Server Suite releases:

ArcSight Versions	Centrify Server Suite Releases
Enterprise Security Manager (ESM) 6.8.0	2016
ESM Console 6.8.0	2016.1 2016.2 2017 2017.1 2017.2 2017.3

ArcSight Components

The following diagram illustrates the ArcSight components that interact with the Centrify Add-on for ArcSight:

Overview of the Integration Steps

The general integration steps that you perform are as follows:

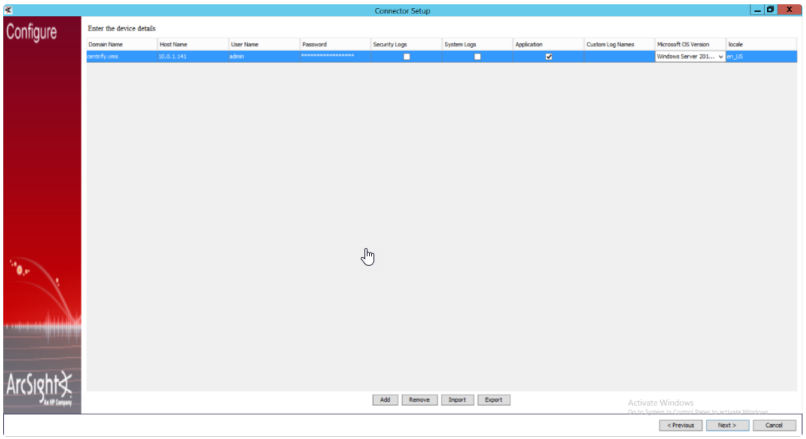
1. Collect Centrify event data from the Windows or Linux machine and forward it to the ArcSight ESM. You must install the ArcSight SmartConnector in the respective environment. (See "ArcSight SmartConnector Installation" below)
2. After successfully installing the ArcSight SmartConnector, place the properties file and the categorizer file in the appropriate location. (See "Configuring FlexConnector for Data Normalization and Categorization" on page 1143)
3. Open the ArcSight Console and the active channel that corresponds to the site connector. You should be able to view the real-time events being received in the active channel on the Windows or Linux machine. (See "Verifying Your Configuration" on page 1144)

ArcSight SmartConnector Installation

Follow the detailed steps in the ArcSight SmartConnector User Guide to install the ArcSight SmartConnector:

https://www.microfocus.com/documentation/arcsight/arcsight-smartconnectors/

Note: As you install the ArcSight SmartConnector, make sure that you only select the Application check box to capture the Application logs.



connector setup

Data Collection from a Windows Agent

Delinea software logs events in the Application logs on Windows machines. To capture the Application logs, Delinea uses the ArcSight SmartConnector for Windows.

There are a number of ways to collect data from Windows machines.
Some of the supported options include:

- Data collection from a stand-alone Windows machine:

Application logs are collected on a stand-alone Windows machine and parsed using the FlexConnector parser. Parsed events are forwarded to the ArcSight ESM where all of the data from Delinea Server Suite is stored, and the ArcSight Console is used to access that data.

- Data collection using the Windows Event Forwarding (WEF) feature:

ArcSight SmartConnector supports WEF to collect Application logs forwarded by several Windows machines to a central machine. You install the ArcSight SmartConnector only on the central Windows machine that received the forwarded events and enable the WFE while installing the ArcSight SmartConnector.

- Data collection using the Active Directory (AD) Source:

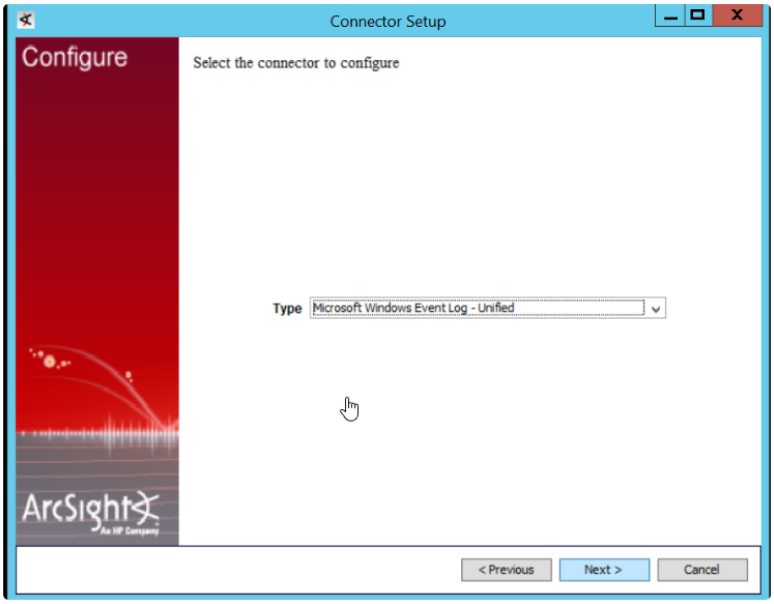
ArcSight SmartConnector supports log collection for all of the member machines from the Active Directory Source itself. You install the ArcSight SmartConnector only on the AD server. During installation, you provide the Domain Controller name and its credentials. If the credentials and the domain name are correct, a list of all the member machines of that Domain Controller are seen in a new window. Users select only those Windows machines from which they want to collect Application logs.

Installing the ArcSight SmartConnector on a Windows Agent

To install ArcSight SmartConnector on a Windows agent:

1. Execute the ArcSight SmartConnector binary for Windows.
2. Choose an installation folder.

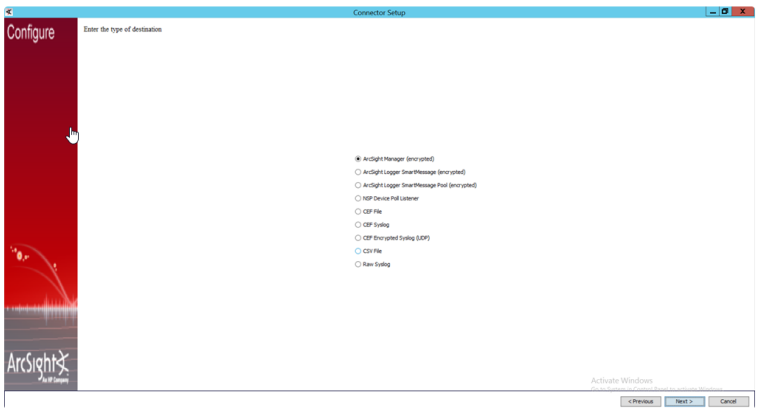
   The default folder is:
   C:\Programme Files\ArcSightSmartConnectors
3. Wait for the installation to complete.



connector setup

4. When you are prompted to select the connector to configure, select Microsoft Windows Event Log – Unified and click Next.
5. If you want to use Windows Event Forwarding, select Enable WEF.

   Note: You can also provide your Active Directory server parameters to get a list of all member VMs, and then select only those Windows machines from which you want to collect Application logs. As you are only installing on a stand-alone machine at this point, leave all of these parameters blank.
6. For the browser type, select Enter Devices Manually (do not use AD Source here).
7. Enter your host details.
   - Make sure that you only select the Application check box to capture the Application logs because Delinea audit trail events are only stored in the Windows Application logs.



- Connector setup

8. When you are prompted for the type of destination, select ArcSight Manager (encrypted).
   - You select ArcSight Manager (encrypted) because Delinea is forwarding the collected logs to the ArcSight ESM.
9. Provide your ArcSight ESM details:
   - Enter the following information for the machine where the ArcSight ESM is installed:
     - Hostname
     - Port
     - Username
     - Password
10. Provide a name for your ArcSight SmartConnector.

    To assist you in assigning an applicable name, understand that the name is displayed on the ArcSight Console to identify those SmartConnector events that the console is receiving.
11. (Optional) If you want to use your ArcSight ESM certificate, select Import Certificate from your ArcSight ESM.
12. Specify whether you want to install the ArcSight SmartConnector as a service or as a stand-alone application.
    - Install as a Service is generally preferred.

Data Collection from a Linux Agent

Delinea software logs events in the syslog directory on Linux machines. To collect the Linux syslog messages, choose from these options:

- Data collection from a stand-alone Linux machine:

To collect syslog messages from stand-alone Linux machines, use the Syslog File type of connector. You provide the directory location for syslog collection. Make sure that you have access to the syslog directory to avoid the error: permission denied.

- Data collection using the Syslog Daemon on a central Linux machine:

The Syslog Daemon type of connector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows.

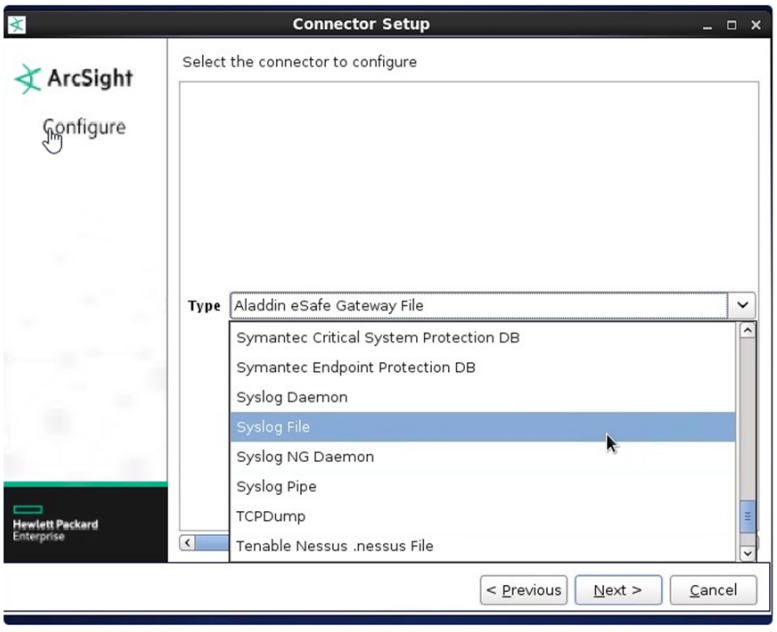
The SmartConnector for the Syslog Daemon implements a UDP receiver on port 514 (the default; which can also be configured) that can be used to receive syslog events. Use of the TCP protocol or a different port can be configured manually. You can forward the syslog from multiple Linux agents to a single machine. For example, when you configure the Syslog Daemon Connector on the 514 UDP port, you need to specify the receiving syslog port (514) and the protocol (UDP).

Installing the SmartConnector on a Linux Agent

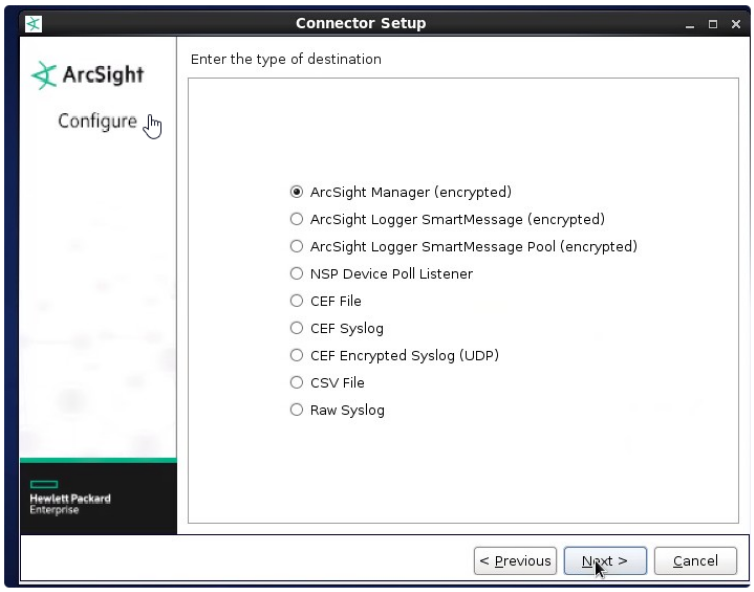
To install the SmartConnector:

1. Execute the SmartConnector binary for Linux.

1. Use the default name for the home folder.
2. Wait for the installation to complete.
3. When you are prompted to select the connector to configure, select Syslog File.



4. Enter the file or directory of the syslog that you want to monitor.
5. When you are prompted to enter the type of destination, select ArcSight Manager (encrypted) and click Next.

- 

  - arcsight manager
  - You select ArcSight Manager (encrypted) because Delinea is forwarding the collected logs to the ArcSight ESM.

6. Provide your ArcSight ESM details.
   - Enter the following information for the machine where the ArcSight ESM is installed:
     - Hostname
     - Port
     - Username
     - Password
7. Provide a name for your ArcSight connector.
   - To assist you in assigning an applicable name, understand that the name is displayed on the ArcSight Console to identify those SmartConnector events that the console is receiving.
8. (Optional) If you want to use your ArcSight ESM certificate, select Import Certificate from your ArcSight ESM.
9. After the installation, check the status of the ArcSight SmartConnector service using following command:
   - /etc/init.d/arc_syslog_file status

Configuring FlexConnector for Data Normalization and Categorization

When the ArcSight SmartConnector has been installed and configured to collect Centrify logs, the logs must be parsed and categorized using a customized Centrify FlexConnector. This FlexConnector contains two files for each Windows and Linux platform: a Parser and a Categorizer. You must place these files at specific locations depending on the operating system (OS) that you are using. Refer to the section below that applies to your OS.

Windows Application Logs

Windows Application Logs

The two files needed for parsing and categorizing Windows application logs are in the folder:

Centrify_windows_flexconnector:

- The Categorizer file is: centrify_suite.csv
- The Parser file is: application.centrify_audittrail_v2.sdkkeyvaluefilereader.properties

To configure the Application logs for Windows:

1. Paste the Categorizer file, centrify_suite.csv, into the target location: $ARCSIGHT_HOME\current\user\agent\acp\categorizer\current\centrify\
2. Paste the Parser file: application.centrify_audittrail_v2.sdkkeyvaluefilereader.properties into the target location for your OS, as indicated by the following table:

Microsoft OS Version	Parser File Location
Windows Server 2008 R2Windows 7 SP1	$ARCSIGHT_HOME\user\agent\fcp\windowsfg\windows_2008
Windows Server 2012Windows Server 2012 R2 Windows 8	$ARCSIGHT_HOME\user\agent\fcp\windowsfg\windows_2012
Windows Server 2016Windows 10	$ARCSIGHT_HOME\user\agent\fcp\windowsfg\windows_2016

|

3. Restart the SmartConnector service from the Windows Services

Linux Syslogs

The two files needed for parsing and categorizing the Linux syslog are in the folder:

Centrify_linux_flexconnector

The two files are:

- Categorizer file: centrify_suite.csv
- Parser file:centrify.subagent.sdkrfilereader.properties

To configure syslogs for Linux:

1. Paste the Categorizer file, centrify_suite.csv, into the target location: $ARCSIGHT_HOME/current/user/agent/acp/categorizer/current/Centrify/
2. Paste the Parser file, centrify.subagent.sdkrfilereader.properties, into the target location, $ARCSIGHT_HOME/user/agent/flexagent/syslog/, regardless of the Linux version.
3. Restart the SmartConnector service from /etc/init.d

Verifying Your Configuration

After you finish configuring the FlexConnectors, Delinea recommends that you verify your configuration to make sure that events from Delinea are parsed correctly through the FlexConnectors.

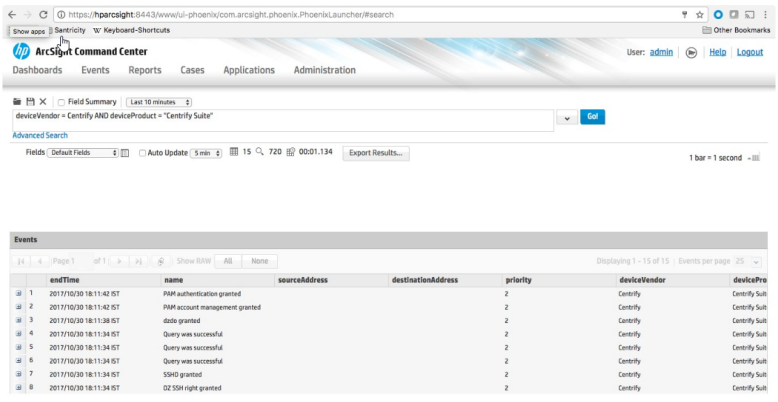
To verify your configuration, generate some login events and then look for them either in the ESM Command Center or on the ESM Console.

ESM Command Center

To look at login events using the ESM Command Center:

1. Generate login events.
2. Log in to the ESM Command Center.
3. Go to Events > Event Search.
4. Search for deviceVendor="Centrify" and deviceProduct="Centrify Suite".

   You should see all the authentication events as shown in the following example:

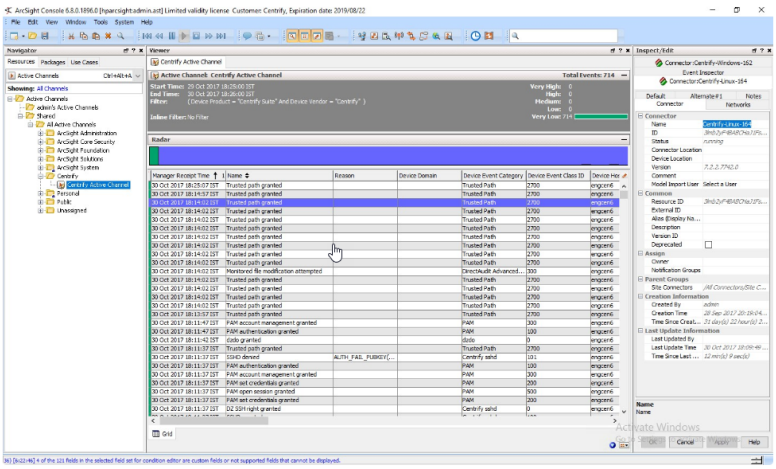


ESM Console

To look at login events using the ESM Console:

1. Generate login events.
2. Log in to the ESM Console.
3. Go to Active Channels > Shared > All Active Channels > Centrify > Centrify Active Channels.

   You should see all of the Centrify audit events as shown in the following example:



Integration with ArcSight CEF

The *Delinea PAS Events and ArcSight CEF Guide* is written to provide detailed instructions for accessing events from the Delinea PAS using REST APIs. The guide also presents instructions for creating ArcSight Common Event Format (CEF) Delinea PAS events.

Overview of the Steps for Accessing Delinea PAS Events

The general steps that you perform to access Delinea PAS events are as follows:

1. As a prerequisite to accessing Delinea PAS events, configure the tenant for OAuth access to create:
   - SIEM user
   - OAuth app
   - SIEM scope for accessing Redrock and query
2. Generate the basic authorization token.
3. Fetch the OAuth access token using the oauth2/token API.
4. Fetch the Delinea PAS events using the Redrock/query API.
5. Parse the response that was received from the Redrock/query API.

Prerequisite for accessing Delinea PAS events

The first task that you must perform before accessing Delinea PAS events is to configure the OAuth tenant. For detailed steps, see "Setting Up the SIEM User and the OAuth App on the Tenant" on the next page. After you complete the configuration, you will have created the following:

- SIEM user
- OAuth app
- SIEM scope for accessing Redrock and query

Setting up the SIEM user and the OAuth app on the tenant

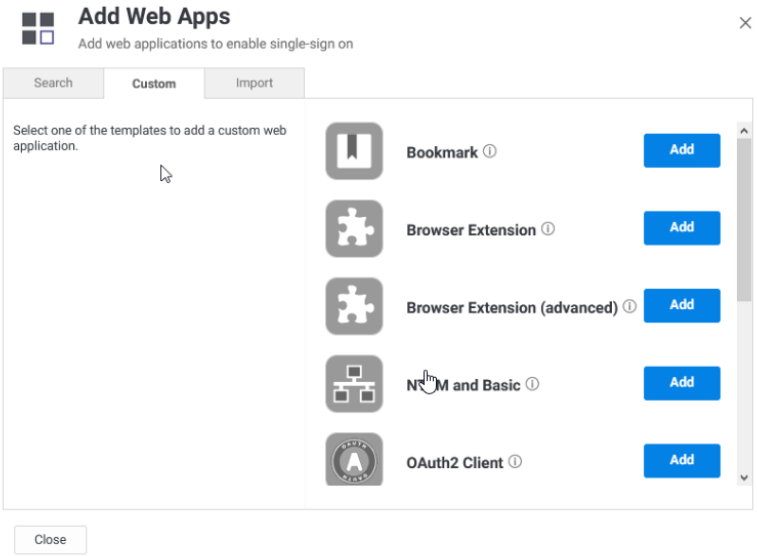
To set up the SIEM user and OAuth app

1. In the Admin Portal, open the **Apps** tab and click **Web Apps**.
2. Click **Add Web Apps**.
3. Select the **Custom** tab and click **Add** for OAuth2 Client.

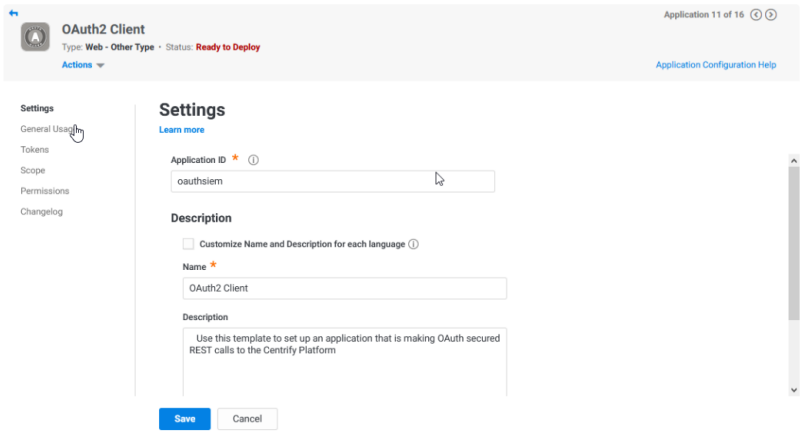
Setting Up the SIEM User and the OAuth App on the Tenant

To set up the SIEM user and OAuth app:

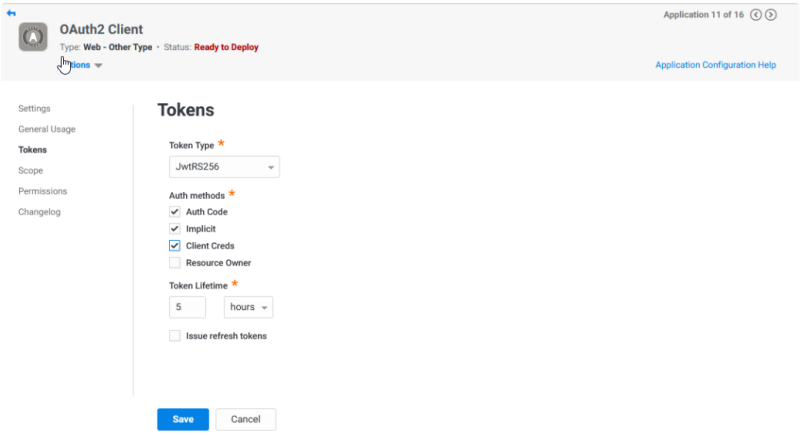
1. In the Admin Portal, open the **Apps** tab and click **Web Apps**.
2. Click **Add Web Apps**.
3. Select the **Custom** tab and click **Add** for OAuth2 Client.



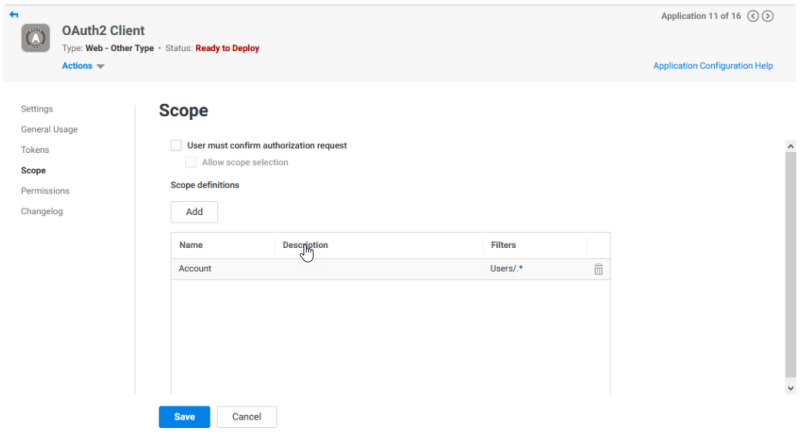
4. When prompted to add the OAuth2 Client web app, click **Yes**
5. Navigate back to the Web Apps screen and click **OAuth2 Client** to open the app.
6. On the Settings tab, enter **oauthsiem** for the Application ID



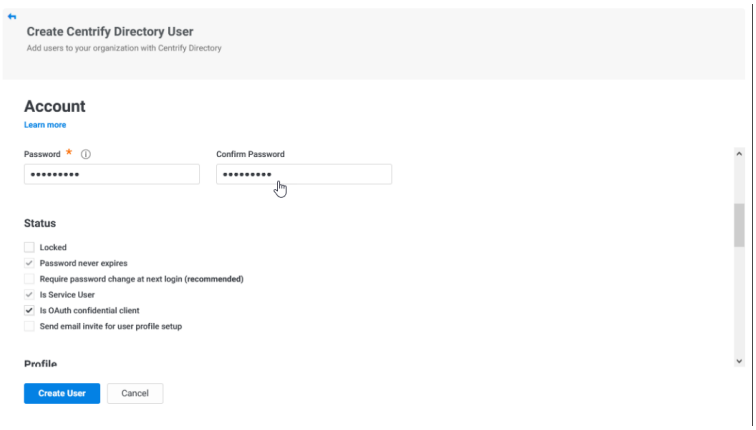
7. On the **General Usage** tab, leave the defaults as shown
8. On the Tokens tab, under Auth methods, check **Client Creds**



9. On the Scope tab, under Scope definitions, click **Add** to add a new scope



10. On the Scope definitions dialog:
    a. In the Name field, enter **siem**.
    b. Under Allowed REST APIs, click **Add,** and enter **Redrock/query**.
    c. Click **Save**.
11. Click **Save** to save the OAuth2 Client changes.
12. From the main menu, open **Access** and select the **Users** tab.
13. Click ***Add User** to add a new user.
14. On the Create Delinea Directory User page, fill out the following fields:
    a. For the Login Name, enter **siemuser**.
    b. For the Suffix, select **centrify.com** (or leave as is).
    c. For Email Address and Display name, enter the user's email address and full name.
    d. Scroll down to the other account fields:



    e. For the Password and Confirm Password, enter the password of your choice. The password must be between 4 to 64 characters long and contain at least one digit.

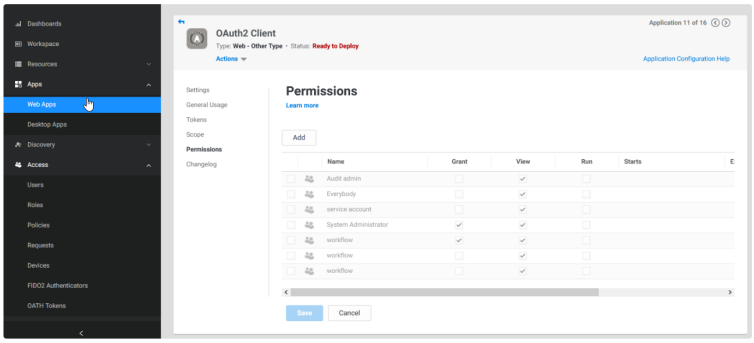
f. Under Status, check **Is OAuth confidential client**. This selection should automatically check **Password never expires**.

g. Click **Create User** to create the new user.

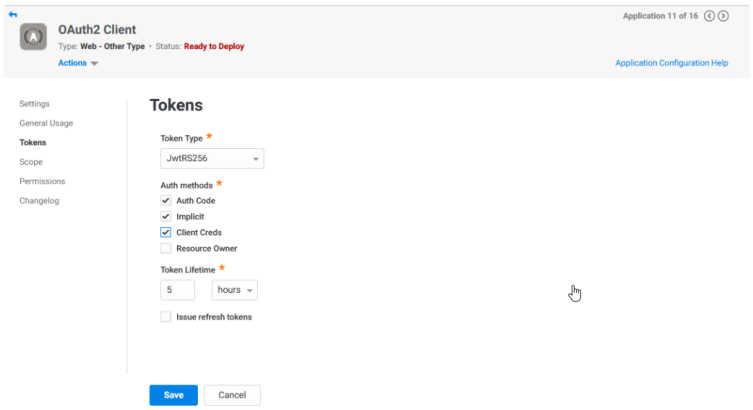
15. From the main menu, select the **Roles** tab and click **Add Rule**.
16. On the service account page:
    a. On the Description tab enter: **service account** for the Name field. This entry serves as the role name.
    b. On the Members tab, search for the **siemuser** that you created earlier and select its checkbox to add the new member.
    c. Click **Add**.
17. On the Administrative Rights page, click **Add** to open the Add Rights list.
18. Check **Read Only System Administration** and click **Add**.
19. Check **Read Only System Administration** and click **Save**.
20. Perform final checks to ensure:
    - On the Users tab, the **siemuser** is shown.

      Note: You may need to check **All Users** to ensure you are shown the full list of users.

    - When you select **siemuser** and click on the **Roles** section, **service account** is listed.
    - Select **Web Apps** > **OAuth2 Client** > **Permissions** . Ensure the permissions for the **service account** role is shown.



- Select the **Tokens** tab and ensure **Client Creds** is checked under Auth methods.



Generating a Basic Authorization Token

To generate a basic authorization token, use the following command:

```
echo -ne "<siem_user>:<password>" | base64
```

Example

Review the following example:

```
echo -ne siemuser@centrify.com:Pass@2k17" | base64
```

Sample Output

The sample output looks like this:

```
c2llbXVzZXJAY2VudHJpZnkuY29tOkxlZW5hQDIwMTc
```

Fetching Events by Using the Redrock/Query API

Use the curl command and the OAuth access token extracted in the previous step:

```
curl  -H "Authorization: Bearer <oauth_access_token>" -H "X-CENTRIFY-NATIVE-CLIENT:True -d
'{"Script":"<query>"}' https://<tenant>/Redrock/query
```

Sample Curl Commands

This sample curl command fetches events for the last 24 hours:

```
curl  -H "Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ijk5QzA4QjQzMjk4NOZDQjRCNOE5MTEwMTdDMTI3QzA4NT
ZCMjAxQzkiLCJ4NXQiOiJtY0NMUXltSF9MUzNxUkVCZkJKOENGYXlBY2siLCJhcHBfaWQiOiJvYXVOaHNpZW0ifQ.e
yJpYXQiOjE1MjE2OTkzNzgsInVuaXF1ZV9uYW1lIjoic2llbXVzZXJAY2VudHJpZnkuY29tIiwiZXhwIjoxNTIxNzE
3Mzc4LCJzdWIiOiI0NDZjOTc5Ni1lOWE4LTRiMDgtYmJkZiO2ZGZlNTJiOGRkOTIiLCJzY29wZSI6InNpZW0ifQ.e5
oE58CxvOqkIb1Z-nCXyhbIxcL_6Bs3znVVyBG6aFb6oHSlb_
y5pPnWaLfQdmfnx6hyHtMOGGRoK6HTVJulSbrCFzqHKBHoW38YPh5M7IzTJflJ-
8kOip9we3ElWm2QiOcbR8AmULYaDR8OnvpIVtmBJ2ZBJng9oFippwoNtBi2gYFjjJsGtRClpqvlHrTytPAqe3SvMOw
hm8yfbq8YhIapcdk_mfJl2YEPX_pyl-Kxzyz9_nHw-_jmOLXzMazvPiAz-
sFCrc8ngtzQZgvDe1wUnPqqEiBOG2Hg2-NCPYi9hcR8OUyeKD4erkgyXRq1KvvrS7G9iLHT1VrLSuOo2g" -H "X-
CENTRIFY-NATIVE-CLIENT:True" -d '{"Script":"Select * from Event where WhenOccurred >
datefunc('\''now'\'', '\''-1'\'')"}' https://aaa0056.my-dev.centrify.com/Redrock/query
```

This sample curl command fetches events between two timestamps:

```
curl  -H "Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ijk5QzA4QjQzMjk4NOZDQjRCNOE5MTEwMTdDMTI3QzA4NT
ZCMjAxQzkiLCJ4NXQiOiJtY0NMUXltSF9MUzNxUkVCZkJKOENGYXlBY2siLCJhcHBfaWQiOiJvYXVOaHNpZW0ifQ.e
yJpYXQiOjE1MjE2OTkzNzgsInVuaXF1ZV9uYW1lIjoic2llbXVzZXJAY2VudHJpZnkuY29tIiwiZXhwIjoxNTIxNzE
3Mzc4LCJzdWIiOiI0NDZjOTc5Ni1lOWE4LTRiMDgtYmJkZiO2ZGZlNTJiOGRkOTIiLCJzY29wZSI6InNpZW0ifQ.e5
oE58CxvOqkIb1Z-nCXyhbIxcL_6Bs3znVVyBG6aFb6oHSlb_
y5pPnWaLfQdmfnx6hyHtMOGGRoK6HTVJulSbrCFzqHKBHoW38YPh5M7IzTJflJ-
8kOip9we3ElWm2QiOcbR8AmULYaDR8OnvpIVtmBJ2ZBJng9oFippwoNtBi2gYFjjJsGtRClpqvlHrTytPAqe3SvMOw
hm8yfbq8YhIapcdk_mfJl2YEPX_pyl-Kxzyz9_nHw-_jmOLXzMazvPiAz-
sFCrc8ngtzQZgvDe1wUnPqqEiBOG2Hg2-NCPYi9hcR8OUyeKD4erkgyXRq1KvvrS7G9iLHT1VrLSuOo2g" -H "X-
CENTRIFY-NATIVE-CLIENT:True -d '{"Script":"Select * from Event where WhenOccurred >=
'\''2018-03-15T11:33:59.273000Z'\'' and  WhenOccurred < '\''2018-03-
21T11:33:59.273000Z'\''"}' https://aaa0056.my-dev.centrify.com/Redrock/query
```

Parsing the Response Received From Redrock/Query

Refer to the following sample Python code to extract events data from a response:

```
import json
response_json = json.loads(response.text)
events = response_json['Result']['Results']
headers = []
for column in response_json['Result']['Columns']:
    headers.append(column['Name'])

for idx, event in enumerate(events):
    print('\n Row Number:' + str(idx))
    for header in headers:
        if event['Row'][header] is not None:
            print(header + "=" + str(event['Row'][header]))
```

References

For additional information, see:

- Delinea Integrations Documentation
- Use Queries

ArcSight CEF format

The Common Event Format (CEF) standard format, developed by ArcSight, enables vendors and their customers to quickly integrate their product information into ArcSight ESM.

CEF defines a syntax for log records comprised of a standard header and a variable extension, formatted as key-value pairs.

When syslog is used as a transport mechanism, CEF uses the following format, comprised of a syslog prefix, a header, and an extension:

Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device Version|Device Event Class ID|Name|Severity|[Extension]

The following example illustrates a general CEF message using syslog transport:

Sep 19 08:26:10 host CEF:0\|Centrify\|Centrify_Cloud\|1.0\|Cloud.core\|Cloud.core.MfaSummary\|5\|src=10.0.0.1 dst=2.1.2.2 spt=1232

Using CEF Without Wyslog

Syslog applies a syslog prefix to each message, no matter what device it arrives from, which contains the date and hostname:

Jan 18 11:07:53 host CEF:Version\|…

However, if an event producer is unable to write syslog messages, it is still possible to write the events to a file. In this case, begin the message with the format shown below, and omit the syslog prefix:

CEF:Version|Device Vendor|Device Product|Device Version|Device Event Class ID|Name|Severity|[Extension]

<!--

Sample Python functions for CEF creation

This section describes a set of sample Python functions for generating CEF-formatted CP events.

There are three main functions in this package:

- fetch_oauth_token()
- query_events()
- cef_generator()

Using the functions to demonstrate sample usage

Prerequisite: Python 3.5 or above

Follow these steps:

1. Download the Python code from https://github.com/centrify/centrify-hparcsight-integration-sample/

2. Install pip packages in requirement.txt.
3. Provide the values for tenant, siem_username, and siem_password in config.ini.
4. Execute sample_usage.py to generate CEF-formatted CP events for one hour:

- python3.5 sample_usage.py

The following example shows a CEF message for a Self-Service App Launch CIS Event:

CEF:0|Centrify|Centrify_Cloud|1.0|Cloud.Saas.Application|Cloud.Saas.Application.SelfServiceAppLaunch|5|dhost=AAA0056 duser=cloudadmin@persistent.com01 msg=User cloudadmin@persistent.com01 launched Instagram from 103.6.32.100 shost=103.6.32.100 src=103.6.32.100 rt=1525844566655 deviceProcessName=centrify-syslog-writer dvchost=dinesh-VirtualBox dtz=Africa/Abidjan requestContext=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36 Edge/15.15063 externalId=772a4a904e82da87.W00.0315.1aa20afe647f09c dpriv=WebRole destinationServiceName=CDS suid=c2c7bcc6-9560-44e0-8dff-5be221cd37ee cs1=Instagram cs1Label=applicationId cs2=Instagram cs2Label=applicationName cs3=Web cs3Label=applicationType cs4=103.6.32.100 cs4Label=clientIPAddress cs5=65f79bb1-4f91-4496-9991-d148da16cc3e cs5Label=internalSessionId cs6=0d10a24f4c57434198fb3ad4559cc48b cs6Label=azDeploymentId directoryServiceNameLocalized=Centrify Directory threadType=RestCall azRoleId=WebRole_IN_0 internalTrackingID=d3a0713b610146ca916155efca2be690 authMethod=UserPassword requestIsMobileDevice=False directoryServiceUuid=09B9A9B0-6CE8-465F-AB03-65766D33B05E requestDeviceOS=Windows level=Info

You can customize the usage or the APIs per your application needs.

Note: CEF has a predefined set of keys.

CEF Mapping of CP Events

This section provides detailed information about how the CEF fields have been mapped from the CP event fields in the Python application described above.

CEF header

Header Field	CP Event Field
Version	'0'
Device Vendor	'Centrify'
Device Product	'Centrify_Cloud'
Device Version	'1.0'
Device Event Class ID	Variable – depends on the event. For example: 'Cloud.Saas.Application'

Header Field	CP Event Field
Name	Variable – depends on the event. For example: Cloud.Saas.Application.SelfServiceAppLaunch'
Severity	Variable – depends on the Level field in event. For example: '5' for Info, '10' for Error.

CP ArcSight CEF extension

The CEF Extension contains a collection of key-value pairs. The keys are predefined and are referred to as the ArcSight Extension Dictionary. (CEF Fields)

Common properties in CP events

This section lists the CEF field mapping of CP events, which are part of the CEF extension.

These properties are common to all events of Cloud Suite and Privilege Services.

ArcSight CEF Field	CP Event Field
The common properties are those listed below in bold.	
Destination Host Name	Tenant
Destination User Name	NormalizedUser
Message	EventMessage
Source Host Name	RequestHostName
Source Address	FromIPAddress
Device Receipt Time	whenoccurred_epoch_ms (This is the event timestamp in UTC)
Device Process Name	'centrify-syslog-writer' (can be configured in cef_mapping.ini)
Device Host Name	Hostname of machine running the python app
Device Time Zone	'Africa/Abidjan' Note: This time zone is chosen mainly to set UTC offset to 0

ArcSight CEF Field	CP Event Field
The keys in the common properties section below are added in the CEF message only if no event-specific CEF mapping is specified for an event in the mapping configuration file, which is enclosed with the Sample Python application for CEF creation.	
Device Custom String 1	AuthMethod
Device Custom String1 Label	'authMethod'
Device Custom String2	RequestIsMobileDevice
Device Custom String2 Label	'requestIsMobileDevice'
Device Custom String3	DirectoryServiceUuid
Device Custom String3 Label	'directoryServiceUuid'
Device Custom String4	RequestDeviceOS
Device Custom String4 Label	'requestDeviceOS'
Device Custom String5	Level
Device Custom String5 Label	Level
-->	

Event-specific properties in CP

This section lists the event-specific properties mapped to ArcSight Fields. All events (whether they are listed below or not) will have the first nine common properties, identified in the table above, mapped in an ArcSight.CEF message.

Any CEF key appearing in event-specific mapping will override the CEF key mapping in the common properties section. For example, the Cloud.Server.ManualAccount.SessionStart event, Destination host (Dhost), and Destination User(duser) will be ‘ComputerName’ and ‘AccountName’, which will overwrite the common properties mapped for dhost and duser.

EventType=Cloud.Core.MfaSummary

ArcSight CEF Field	CP Event Field
Reason	MfaReason
Outcome	MfaResult

ArcSight CEF Field	CP Event Field
RequestContext	RequestUserAgent
ExternalId	ID
Dpriv	AzRoleName
DestinationServiceName	DirectoryServiceName
Device Custom String 1	MfaInitiator
Device Custom String1 Label	‘mfaInitiator’
Device Custom String2	FactorsLocalized
Device Custom String2 Label	‘factorsLocalized’
Device Custom String3	ProfileName
Device Custom String3 Label	‘profileName’
Device Custom String4	FailReason
Device Custom String4 Label	‘failReason’
Device Custom String5	MfaUnlock
Device Custom String5 Label	‘mfaUnlock’
Device Custom String6	ForgotPassword
Device Custom String6 Label	‘forgotPassword’
Device Custom Number1	Factorcount
Device Custom Number1 Label	‘factorCount’
Device Custom Number2	SecurityQuestionAnswerCount
Device Custom Number2 Label	‘securityQuestionAnswercount’

Note: The remaining fields in an event that are not mapped to CEF keys will still be added in the CEF message with their CP-event field keys. These custom non-CEF keys will not be available for reporting in ArcSight, but they can viewed as part of the raw event message.

EventType=Cloud.Saas.Application.AppLaunch

ArcSight CEF Field	CP Event Field
RequestContext	RequestUserAgent
ExternalId	ID
Dpriv	AzRoleName
DestinationServiceName	DirectoryServiceName
Suid	UserGuid
Device Custom String 1	ApplicationID
Device Custom String1 Label	‘applicationId’
Device Custom String2	ApplicationName
Device Custom String2 Label	‘applicationName’
Device Custom String3	ApplicationType
Device Custom String3 Label	‘applicationType’
Device Custom String4	TemplateName
Device Custom String4 Label	‘templateName’
Device Custom String5	InternalSessionId
Device Custom String5 Label	‘internalSessionId’
Device Custom String6	AzDeploymentId
Device Custom String6 Label	azDeploymentId

EventType=Cloud.Saas.Application.GatewayAppLaunch

EventType=Cloud.Saas.Application.SelfServiceAppLaunch

ArcSight CEF Field	CP Event Field
RequestContext	RequestUserAgent
ExternalId	ID

ArcSight CEF Field	CP Event Field
Dpriv	AzRoleName
DestinationServiceName	DirectoryServiceName
Suid	UserGuid
Device Custom String 1	ApplicationID
Device Custom String1 Label	‘applicationId’
Device Custom String2	ApplicationName
Device Custom String2 Label	‘applicationName’
Device Custom String3	ApplicationType
Device Custom String3 Label	‘applicationType’
Device Custom String4	ClientIPAddress
Device Custom String4 Label	‘clientIPAddress’
Device Custom String5	InternalSessionId
Device Custom String5 Label	‘internalSessionId’
Device Custom String6	AzDeploymentId
Device Custom String6 Label	azDeploymentId

EventType=Cloud.Server.ManualAccount.SessionStart

EventType= Cloud.Server.LocalAccount.SessionStart

ArcSight CEF Field	CP Event Field
Src	FromIPAddress
Suser	NormalizedUser
Dhost	ComputerName
Duser	AccountName
RequestContext	RequestUserAgent

ArcSight CEF Field	CP Event Field
ExternalId	ID
Dpriv	AzRoleName
DestinationServiceName	DirectoryServiceName
Suid	UserGuid
Device Custom String 1	UserType
Device Custom String1 Label	‘userType’
Device Custom String2	SessionType
Device Custom String2 Label	‘sessionType’
Device Custom String3	AuthorityName
Device Custom String3 Label	‘authorityName’
Device Custom String4	JumpType
Device Custom String4 Label	‘jumpType’
Device Custom String5	DirectoryServiceNameLocalized
Device Custom String5 Label	‘directoryServiceNameLocalized’
Device Custom String6	AuthoritySource
Device Custom String6 Label	‘authoritySource’

EventType=Cloud.Server.LocalAccount.PasswordExport

EventType= Cloud.Server.DomainAccount.PasswordExport

ArcSight CEF Field	CP Event Field
Src	FromIPAddress
Suser	NormalizedUser
Dhost	ComputerName
Duser	AccountName

ArcSight CEF Field	CP Event Field
RequestContext	RequestUserAgent
ExternalId	ID
Dpriv	AzRoleName
DestinationServiceName	DirectoryServiceName
Suid	UserGuid
Device Custom String 1	UserType
Device Custom String1 Label	‘userType’
Device Custom String2	AuthorityID
Device Custom String2 Label	‘authorityID’
Device Custom String3	AuthorityName
Device Custom String3 Label	‘authorityName’
Device Custom String4	AzRoleId
Device Custom String4 Label	‘azRoleId’
Device Custom String5	DirectoryServiceNameLocalized
Device Custom String5 Label	‘directoryServiceNameLocalized’
Device Custom String6	CheckedOut
Device Custom String6 Label	‘checkedOut’
Device Custom Date1	WhenDueBack
Device Custom Date1 Label	‘whenDueBack’

EventType=Cloud.Core.Server.CpsTileLaunch

ArcSight CEF Field	CP Event Field
RequestContext	RequestUserAgent
ExternalId	ID

ArcSight CEF Field	CP Event Field
Dpriv	AzRoleName
DestinationServiceName	DirectoryServiceName
Suid	UserGuid
Device Custom String 1	UserType
Device Custom String1 Label	‘userType’
Device Custom String2	ApplicationType
Device Custom String2Label	‘applicationType’
Device Custom String3	ApplicationName
Device Custom String3Label	‘applicationName’
Device Custom String4	ApplicationID
Device Custom String4Label	‘applicationId’
Device Custom String5	DirectoryServiceNameLocalized
Device Custom String5Label	‘directoryServiceNameLocalized’
Device Custom String6	InternalTrackingID
Device Custom String6Label	‘internalTrackingID’

EventType=Cloud.Core.AdaptiveMfa.RiskAnalysis

Only Common properties.

Alternate approach for creating the Common Extension Format (CEF)

In case you are using the CP REST APIs directly in your application and generating your own Cloud Suite syslog messages in a generic non-CEF format having key=value pairs separated by a delimiter, then ArcSight SmartConnector will need to be installed and configured to collect these Cloud Suite syslog.

These logs will need to be parsed into CEF format by creating ArcSight FlexConnector, to enable Cloud Suite events to be usable for SIEM in ArcSight. The only downside to using a FlexConnector is that ArcSight does not officially certify it.

Fetching the OAuth Access Token by Using the Oauth2/Token API

Use the curl command and the basic authorization token extracted in the previous step:

```
curl -H "Authorization: Basic <basic_auth_token>" -H "X-CENTRIFY-NATIVE-CLIENT:True -d
"grant_type=client_credentials&scope=<siem_scope>" https://<tenant>/oauth2/token/<oauth_
app_id>
```

Sample Curl Command

Review the sample curl command:

```
curl -H "Authorization: Basic c2llbXVzZXJAY2VudHJpZnkuY29tOkalZW5hQDIwMTc" -H "X-CENTRIFY-
NATIVE-CLIENT:True -d "grant_type=client_credentials&scope=siem" https://aaa0056.my-
dev.centrify.com/oauth2/token/oauthsiem
Sample Output
```

Sample Output

The sample output looks like this:

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ijk5QzA4QjQzMjk4N0ZDQjRCN0E5MTEwMTdDMTI3QzA4NT
ZCMjAxQzkiLCJ4NXQiOiJtY0NMUXltSF9MUzNxUkVCZkJKOENGYXlBY2siLCJhcHBfaWQiOiJvYXV0aHNpZW0ifQ.e
yJpYXQiOjE1MjE2OTkzNzgsInVuaXF1ZV9uYW1lIjoic2llbXVzZXJAY2VudHJpZnkuY29tIiwiZXhwIjoxNTIxNzE
3Mzc4LCJzdWIiOiI0NDZjOTc5Ni1lOWE4LTRiMDgtYmJkZi02ZGZlNTJiOGRkOTIiLCJzY29wZSI6InNpZW0ifQ.e5
oE58Cxv0qkIb1Z-nCXyhbIxcL_6Bs3znVVyBG6aFb6oHSlb_
y5pPnWaLfQdmfnx6hyHtM0GGRoK6HTVJulSbrCFzqHKBHoW38YPh5M7IzTJflJ-
8k0ip9we3ElWm2QiOcbR8AmULYaDR8OnvpIVtmBJ2ZBJng9oFippwoNtBi2gYFjjJsGtRClpqvlHrTytPAqe3SvM0w
hm8yfbq8YhIapcdk_mfJl2YEPX_pyl-Kxzyz9_nHw-_jm0LXzMazvPiAz-
sFCrc8ngtzQZgvDe1wUnPqqEiB0G2Hg2-NCPYi9hcR8OUyeKD4erkgyXRq1KvvrS7G9iLHT1VrLSu0o2g
```

Introduction to QRadar Integration

The Delinea for QRadar Integration Guide is written to assist Delinea customers with the task of easily integrating event data in Delinea Server Suite with QRadar.

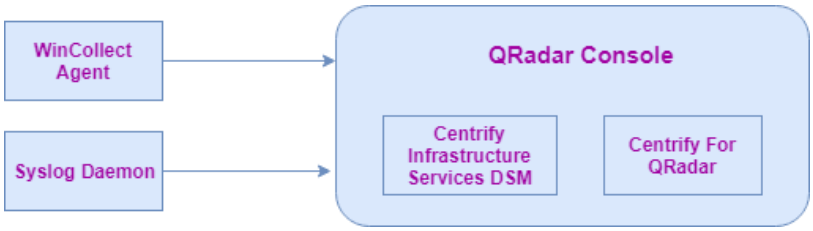
You can leverage the Delinea Add-on for QRadar to normalize Delinea events in QRadar.

This integration guide applies to the following QRadar versions and Delinea Server Suite releases:

QRadar Versions	Centrify Server Suite Releases	
7.2.8 and above	2016	
	2016.1 2016.2 2017 2017.1 2017.2 2017.3	

QRadar Components

The following diagram illustrates the QRadar components that interact with the Delinea Add-on for QRadar:



Important Information About This Guide

Some sections in this document apply to:

- Windows installations only
- *Nix installations only
- All operating systems

In cases where different steps are required for Windows versus *Nix, two separate sections are provided, one for each operating system (OS). In those sections that only pertain to *Nix, Linux examples are used. If you use a different *Nix OS, see the documentation for your system for more information.

WinCollect Agent

The WinCollect agent collects Delinea audit trail events from the Windows machine and forwards them to the QRadar Console. You can download the WinCollect agent from IBM Fix Central at: https://www.945.ibm.com/support/fixcentral/swg/selectFixes?product=ibm%2FOther+software%2FIBM+Security+QRadar+SIEM&fixids=7.2.0-QRADAR-wincollect-7.2.5-27.x64.exe&source=dbluesearch&function=fixId&parent=IBM%20Security

Syslog Daemon

The syslog daemon collects Delinea audit trail events from a Linux machine and forwards them to the QRadar Console.

Delinea Server Suite Device Support Module (DSM)

The Delinea Server Suite DSM collects Delinea events on the QRadar Console. You can get this DSM from: https://www.ibm.com/support/knowledgecenter/en/SS42VS_DSM/c_dsm_guide_Centrify_Server_Suite_overview.html

Delinea Add-on for QRadar

The Delinea Add-on for QRadar (in CentrifyForQRadar.zip) consists of approximately 120 Custom Event Properties for parsing different fields from the Delinea audit trail events. You can get the Delinea Add-on for QRadar from the Delinea web site.

Overview of the Integration Steps

The general integration steps that you perform are as follows:

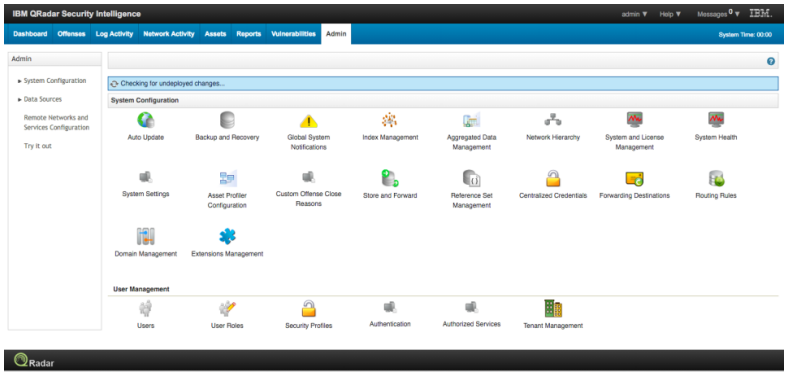
1. Ensure that the QRadar Console is installed and running.
2. "DSM Installation" on page 1170.
3. "Installing Add-on for QRadar" below.
4. "Installation and Configuration for Data Collection" on the next page.
5. "Log Source Configuration" on page 1170.
6. "Verifying your QRadar configuration" on page 1175.

Installing Add-on for QRadar

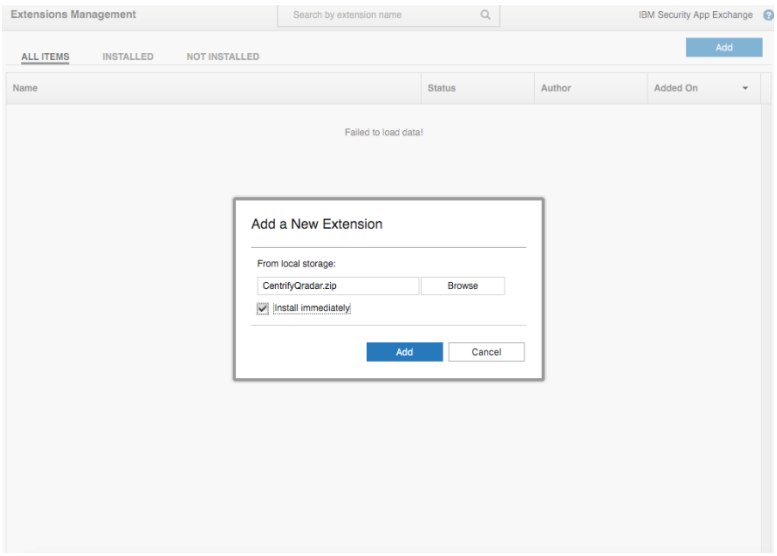
You must ensure that the Delinea Infrastructure Services DSM is installed on QRadar. before installing the Delinea Add-on for QRadar, To check the availability of the DSM, see the Pre-Installation instructions for Windows and *Nix see "Installation and Configuration for Data Collection" on the next page

To download the Delinea Add-on for QRadar:

1. Log in to the QRadar Console using your admin credentials.
2. Go to the Admin tab.



3. Click **Extensions Management**.
4. Choose the downloaded Zip file.



5. Click the checkbox, **Install immediately**, and click **Add**.

   The QRadar Console displays a screen that describes all of the components in detail.
6. Click **OK** to install the application on QRadar.
7. Click **Deploy changes**.

Installation and Configuration for Data Collection

This section describes the steps to:

- Pre-Install the WinCollect Agent on Windows
- Pre-Install Syslog on *Nix
- Install the WinCollect Agent on Windows
- Configure Syslog on Linux

Pre-Installation of the WinCollect Agent on Windows

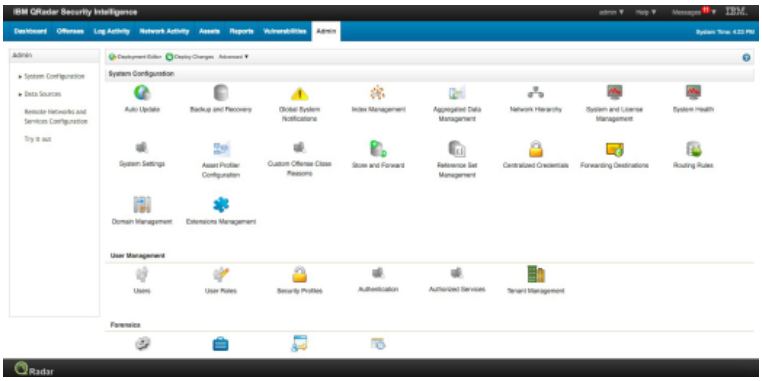
Before you install QRadar on Windows, follow these steps:

1. From the IBM site, download the version of the WinCollect agent for your system type (32-bit or 64-bit).
2. Download the Delinea Add-on for QRadar.
3. Verify the availability of the Delinea DSM for QRadar using this command:

   ```
   rpm –qa | grep –i Centrify
   ```
4. Configure the Authorization Token, which authenticates communication between Windows machines and the QRadar Console:

   a. Log in to the QRadar Console using Admin credentials.

   b. Click the **Admin** tab.

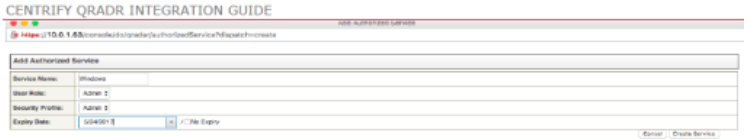
c. 

In the User Management section, click Authorized Services.

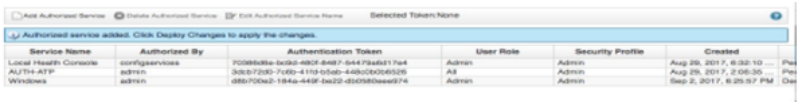
d. Enter the name for the token.

e. Choose **Admin** as **UserRole and Security Profile**.

f. Set the Expiry Date by selecting the No Expiry checkbox.

g. 

Click **Create Service**.



On completion, QRadar creates a token that can be accessed from the QRadar Console.

Pre-Installation of Syslog on *Nix

To prepare for the QRadar installation on a *Nix machine:

1. Ensure that syslog daemon (syslog/rsyslog/syslog-ng) is installed by using the appropriate command (either one below) to verify it:

   ```
   service status rsyslogorservice status syslog-ng
   ```

2. If the syslog daemon is not installed, use the appropriate command (either one below) to install the required syslog daemon:

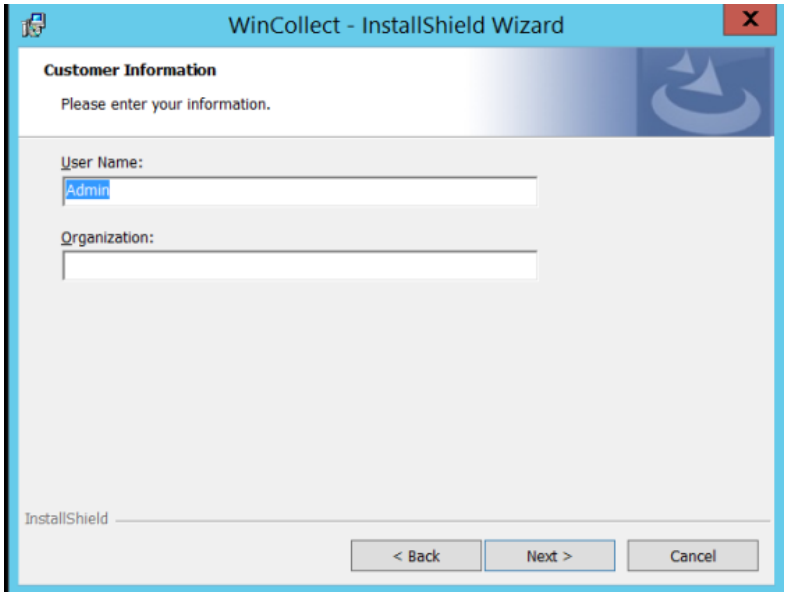
   ```
   yum install rsyslogor

   yum install syslog-ng
   ```

3. Download the Delinea Add-on for QRadar.
4. Check the availability of the Delinea DSM for QRadar:

```
rpm -qa | grep -i Centrify
```

Installing the WinCollect Agent on Windows

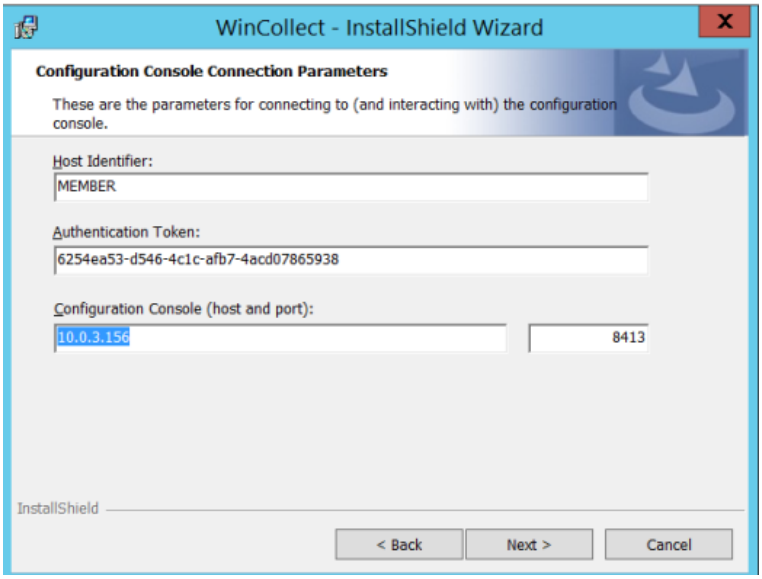
To install the WinCollect Agent on Windows:

1. Right-click the binary and run as administrator.
2. 

Enter the User Name (such as Admin) and Organization and click Next.
3. 

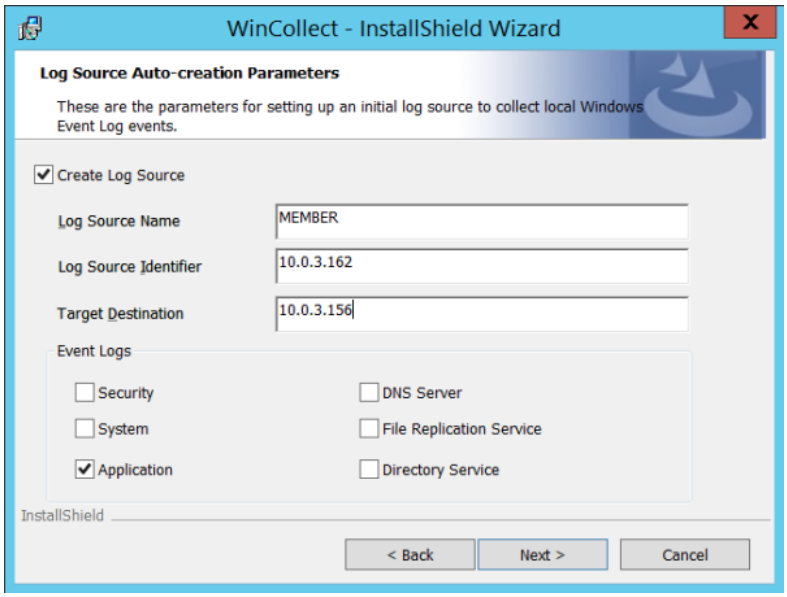
For the Setup type, choose Managed and click Next.
4. Add the following Configuration Console Connection parameters:

- Host Identifier - Hostname in QRadar
- Authentication Token - Generated using the authorized services in QRadar
- Configuration Console (host and port):
- Console IP is the location where QRadar is installed



QRadar communicates with WinCollect agents on ports 8413 and 514 by default, so make sure that these ports are open in the firewall

5. Click Next.
6. Add the following Log Source Auto-creation Parameters:
   - Click the checkbox, Create Log Source
   - Log Source Name - Is provided and appears as a machine name on QRadar
   - Log Source Identifier - IP address of the Windows machine member
   - Target Destination - IP address of the QRadar instance
   - Event Logs - Check Application as Delinea events are audited in the application logs



7. Click Next in the next two screens:
   a. Heartbeat parameters
   b. Installation Parameters summary
8. Click Finish to complete the installation of WinCollect.
9. Navigate to the QRadar Console to deploy the changes.
10. Click **Deploy Changes** to add the new log source on QRadar.

Configuring Syslog on Linux

To configure the Syslog Forwarder to forward events to the QRadar Console:

1. Update the rsyslog.conf file and add the following line:

   ```
   *.* @@Qradar_Console_IP:514
   ```

   This file is available in the /etc folder for RedHat Linux.
   Refer to the OS-specific documentation to find the file location.
2. If you are using syslog-ng, add following entry:

   ```
   #My Switches
   source s_centrify {file("/var/log/messages ");};destination d_tcp { network("QRadarHost"
   port(1999)) ; };log {source(s_centrify) ; destination(d_centrify) ; } ;
   ```

3. Restart the syslog daemon using one of the following commands:

   ```
   service rsyslog restart or
   service syslog-ng restart
   ```

DSM Installation

The Delinea Infrastructure Services DSM is used for parsing events. This DSM is available with the latest version of QRadar. For an existing QRadar installation, you can get the DSM through an automatic update or by manual installation.

Automatic Update

Updates to the DSM, PROTOCOL, and VIS RPMs are made available on a weekly basis to QRadar administrators.

Use the Internet to enable the appliances to connect to an automatic update server:

1. Log in to the QRadar Console as the admin user.
2. Go to Admin > Auto Update to see all the available updates.
3. Choose the appropriate option for your installation.

Manual Installation

To manually install the DSM:

1. Log in to IBM Fix Central and search for the Delinea Infrastructure Services DSM.
2. Download the RPM file from the location specified in the Introduction section.
3. Copy this bundle to the QRadar Console.
4. Log in (SSH) to the QRadar Console and run the following command:
   ```
   rpm –ivh DSM-CentrifyInfrastructureServices-7.3-20171106211603.noarch
   ```
5. If you do not see the DSM named Delinea Infrastructure Services using the command:
   ```
   rpm -qa | grep -i Centrify
   ```
   then download the DSM from the IBM web site.
6. To install the DSM, add the DSM to the QRadar instance using WInSCP and run the following command:
   ```
   yum -y install <rpm_filename>
   ```

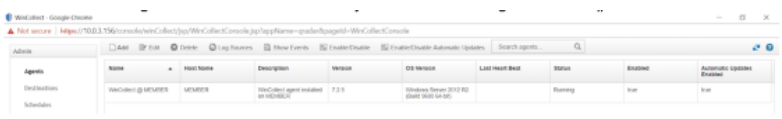
Log Source Configuration

This section provides the log source configuration details for Windows and Linux machines.

Log Source Creation for Windows

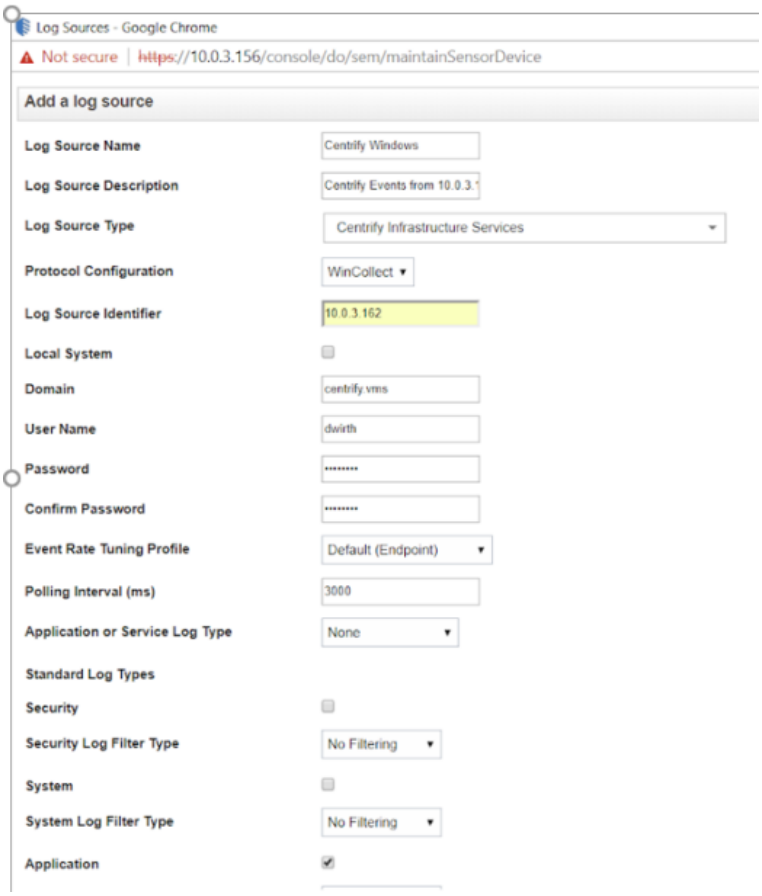
To create a log source on a Windows machine:

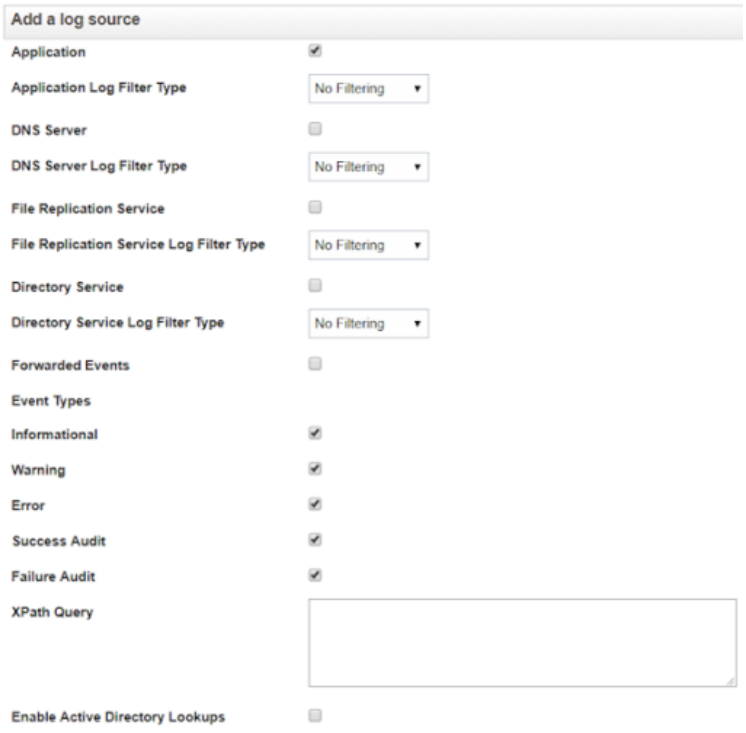
1. In the Admin tab, click WinCollect to see the WinCollect agent that was created.



2. Click **Add a log source** and provide the following information:

- Log Source Name – Example: Delinea Windows
- Log Source Description – Example: Delinea Events from 10.0.3.162
- Log Source Type – Select Delinea Infrastructure Services
- Protocol Configuration – **WinCollect**
- Log Source Identifier – IP address of the machine that is sending events to QRadar. Example: 10.0.3.162
- Domain – **centrify.vms**
- User Name – for the Domain value (such as centrify.vms)
- Password – for the Domain value (such as centrify.vms)
- Standard Log Types – Click **Application**
- WinCollect Agent – Select the **WinCollect @ MEMBER** agent that you created in WinCollect
- Coalescing Events – Deselect (uncheck) it
- Log Source Extension – **Delinea**



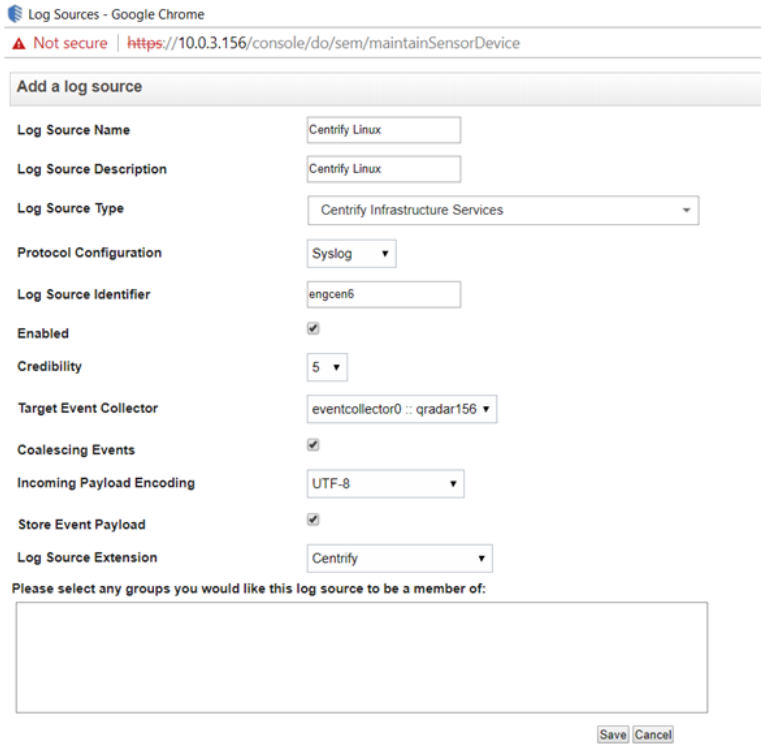

Add a log source
Application
Application Log Filter Type
No Filtering
DNS Server
DNS Server Log Filter Type
No Filtering
File Replication Service
File Replication Service Log Filter Type
No Filtering
Directory Service
Directory Service Log Filter Type
No Filtering
Forwarded Events
Event Types
Informational
Warning
Error
Success Audit
Failure Audit
XPath Query
Enable Active Directory Lookups

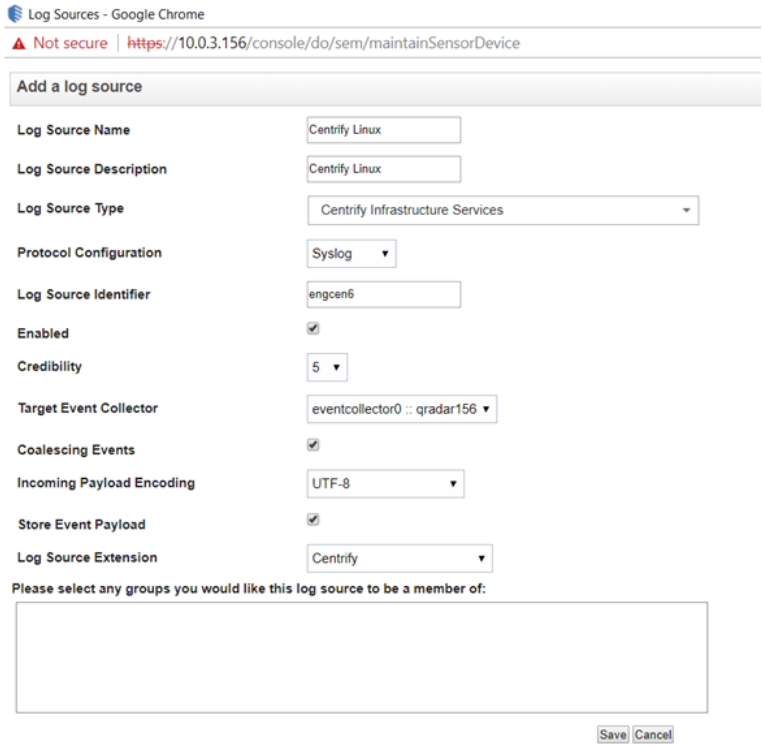
3. Click **Save**.
4. At the prompt, deploy the changes.

Log Source Creation for Linux

To create a log source on a Linux machine:

1. Click **Add a log source.**
2. Provide the following information:
   - Log Source Name – Example: Delinea Linux
   - Log Source Description – Example: Delinea Linux
   - Log Source Type – Select Delinea Infrastructure Services
   - Protocol Configuration – **Syslog**
   - Log Source Identifier – IP address of the machine that is sending events to QRadar. Example: 10.0.3.162
   - Coalescing Events – **Check it**
   - Log Source Extension – Select Delinea


Log Sources - Google Chrome
Not secure
https://10.0.3.156/console/do/sem/maintainSensorDevice
Add a log source
Log Source Name
Centrify Linux
Log Source Description
Centrify Linux
Log Source Type
Centrify Infrastructure Services
Protocol Configuration
Syslog
Log Source Identifier
engcen6
Enabled
Credibility
5
Target Event Collector
eventcollector0 :: qradar156
Coalescing Events
Incoming Payload Encoding
UTF-8
Store Event Payload
Log Source Extension
Centrify
Please select any groups you would like this log source to be a member of:
Save
Cancel



3. Click **Save**.
4. At the prompt, deploy the changes.

Verifying your QRadar configuration

After the installation of the Delinea Add-on for QRadar is complete, QRadar should be parsing and indexing the new Delinea audit trail events.

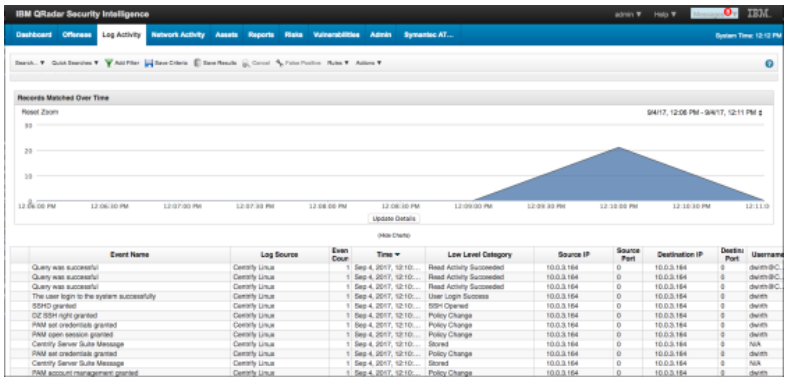
To validate your installation:

1. Generate some Delinea audit trail events into a Delinea managed member server.

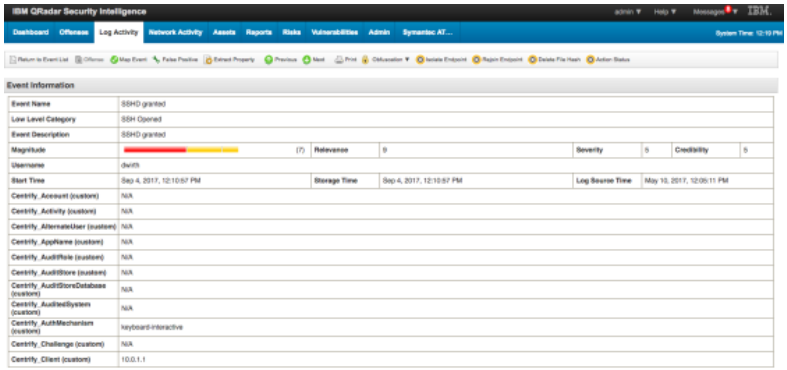
   For example, log in to the server to generate an authentication event. You should be able to access the generated events from the QRadar Console system.

2. Log in to the QRadar Console and click the **Log Activity** tab.

   You should see different Delinea audit events that QRadar parsed.



When you click a specific event to open the detailed view, it should show various Delinea-specific fields as shown in the following example:



Integration with Splunk

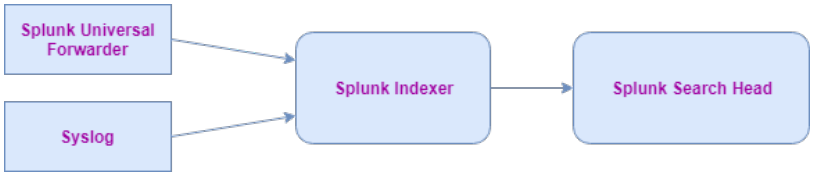
The Delinea for Splunk Integration Guide is written to assist Delinea Privileged Access Service customers with the task of easily integrating event data in Delinea PAS with Splunk. You can leverage the Delinea Add-on for Splunk to normalize Delinea events in Splunk.

This integration guide applies to the following Splunk versions and Delinea PAS releases:

Splunk Versions	Delinea Privileged Access Service Releases
6.5.x	2016
6.6.x. 7.0.0	2016.1 2016.2 2017 2017.1 2017.2 2017.3
8.0	2020.2
8.1	2020.6
8.x	2020.7

Splunk Components

The following diagram illustrates the Splunk components that interact with the Delinea Add-on for Splunk:



Delinea Add-on for Splunk

Add-ons are used in Splunk for data onboarding and parsing. The parsed events can be used for ad-hoc queries or to create visualizations. This Add-on can co-exist with other Splunk Add-ons without conflicts.

The Delinea Add-on for Splunk contains:

- Data inputs for Windows and Unix Delinea agents (disabled by default)
- A Parser to extract all of the Delinea event fields
- Event types to categorize Delinea event categories such as Delinea Configuration, Direct Authorize – Windows, and so on
- Tags so that Delinea authentication data complies with the Splunk Common Information Model (CIM)

Delinea App for Splunk

In general, the apps used in Splunk are mainly those for data visualization such as dashboards and report alerts.

The apps contain:

- Sample Delinea dashboards
- Sample weekly reports
- Sample alerts

Data Collection

Data collection can be accomplished in two ways:

- Using the Splunk Add-on for Windows or the Splunk Add-on for Unix and Linux
- Using the Delinea Add-on for Splunk

Using the Splunk Add-on for Windows or Splunk Add-on for Unix and Linux

If you are already using the Splunk Add-on for Windows and collecting Windows application logs on Indexers, you should already have the Splunk Forwarder and the Splunk Add-on for Windows installed on the Windows machine. Because Delinea logs are already part of the Windows application logs, you do not have to install anything else on the Splunk Forwarder. You should be able to see the Delinea data directly on the Indexers.

Similarly, you might already using the Splunk Add-on for Unix and Linux and sending specific UNIX and Linux logs to the Indexers. In this scenario, the Splunk Forwarder and the Splunk Add-on for Unix and Linux should be

installed on the Unix machine. You can modify the inputs.conf file and add the Delinea-specific log directory and start forwarding that data to the Indexers.

Note that the data collection stanzas in the Delinea Add-on for Splunk remain disabled because they are not collecting data in this scenario. The expectation is that the Splunk Add-on for Windows and the Splunk Add-on for Unix and Linux are responsible for collecting data. In this case, the Delinea Add-on for Splunk is mainly used for field extractions and data normalization.

The requirements for component deployment are listed in the following table:

Machines and Splunk Components

	Windows Machines	Unix Machines	Indexers	Search Heads
Splunk Universal Forwarder	Yes	Yes	---	---
Splunk Add-on for Windows	Yes	---	---	---
Splunk Add-on for Unix and Linux	---	Yes	---	---
Centrify Add-on for Splunk	---	---	Yes (Needed for indexed time field extractions)	Yes (Needed for indexed time field extractions and data normalization)
Centrify App for Splunk	---	---	---	Yes

Using the Delinea Add-on for Splunk

If you do not have the Splunk Add-on for Windows or the Splunk Add-on for Unix and Linux and would like to use the Delinea Add-on for Splunk for data collection, you must install:

- Splunk Forwarder on the Windows and the Unix machines
- Delinea Add-on for Splunk on both types of machines

The **inputs.conf** file in the Delinea Add-on for Splunk contains entries for various file locations for monitoring the syslog depending on the OS platform.

You must enable the corresponding input stanza based on the OS platform. Data gets collected on the Forwarder and is then forwarded to the Indexers where the data gets indexed. Note that data collection stanzas in the inputs.conf file remains disabled on the Search Heads.

Note: If the UNIX and Linux syslogs are stored in binary, you must use the rsyslog daemon service to put logs under any of the standard syslog locations before configuring the app on the Forwarder.

The requirements for component deployment are listed in the following table:

	Machines and Splunk Components			
	Windows Machines	Unix Machines	Indexers	Search Heads
Splunk Universal Forwarder	Yes	Yes	---	---
Centrify Add-on for Splunk	Yes	Yes	Yes (Needed for indexed time field extractions)	Yes (Needed for indexed time field extractions and data normalization)
Centrify App for Splunk	---	---	---	Yes

Overview of the Integration Steps

The general integration steps that you perform are as follows:

1. In a stand-alone environment, install and configure the Delinea Add-on for Splunk and the Delinea App for Splunk on the same machine See "Installation and Configuration for a Stand-Alone Environment" below.
2. For an on-premise deployment, install and configure the Delinea App for Splunk on the Forwarder, Indexer, and Search Head as identified in the previous tables See "Installation and Configuration for an On-Premise Deployment" on page 1181.
3. In a cloud deployment, install and configure the Delinea App for Splunk on the Forwarder, Indexer, and Search Head as identified in the previous tables (See "Installation and Configuration for a Cloud Deployment" on page 1183.

Installation and Configuration for a Stand-Alone Environment

This section describes the steps to:

- Install the Delinea Add-on for Splunk and the Delinea App for Splunk
- Configure the Delinea Add-on for Splunk

Installing the Delinea Add-on for Splunk and the Delinea App for Splunk

To install the Add-on and the App from the command prompt, enter the following commands:

```
$SPLUNK_HOME/bin/splunk install app <span class="global-vars.CompanyName mc-
variable">Delinea</span>-add-on-for-splunk_xxx.tgz

$SPLUNK_HOME/bin/splunk install app <span class="global-vars.CompanyName mc-
variable">Delinea</span>-app-for-splunk_xxx.tgz
```

To install the Delinea Add-on for Splunk and the Splunk app from the UI:

1. Log in to the Splunk web site.
2. Go to: **Manage Apps** > **Install App from File**.
3. Choose `Centrify-add-on-for-splunk_xxx.tgz and Delinea-app-for-splunk_xxx.tgz`, one-by-one, and click install.
4. While selecting the build package, click the checkbox to upgrade the app. |

Configuring the Delinea Add-on for Splunk

To start the data collection, you must configure the Delinea Add-on for Splunk.

To configure the Delinea Add-on for Splunk:

1. Make sure that you have administrator rights on your computer.
2. Copy:
   `$SPLUNK_HOME/etc/apps/TA-centrify/default/inputs.conf.example` to:`$SPLUNK_HOME/etc/apps/TA-centrify/local/inputs.conf.example`.
3. Rename **inputs.conf.example** to **inputs.conf**.
4. Open the **inputs.conf** file in a text editor.
5. Find the input stanza for your OS platform among the input stanzas in **inputs.conf**.
6. To enable the stanza for monitoring the syslog for your OS platform, enable that stanza by changing the disabled property of the stanza from:
   `disabled = 1`
   to:
   `disabled = 0`.
7. Save the **inputs.conf** file.
8. Restart the Splunk app.

> **Note:** If Delinea PAS and Splunk are not installed on the same machine, you must forward Delinea events to the Splunk instance.

To forward Delinea events to the Splunk instance, use the following instructions for the Windows and Linux operating systems.

Windows

On a Windows machine, Delinea events are forwarded through the Splunk Universal Forwarder.

To configure events on Windows with the Delinea Add-on for Splunk:

1. Install the Splunk Universal Forwarder on a machine where the Delinea PAS are installed.
2. While performing the installation, enter the Splunk instance IP address and the port on which you are forwarding data. (Default port is 9997).
3. Install the Delinea Add-on for Splunk on Splunk Universal Forwarder using the following command:

Note: Default username and password is **admin/changeme**

```
$SPLUNK_HOME/bin/splunk install app \<path of Delinea Add-on for Splunk build package\>
```

4. Configure the Delinea Add-on for Splunk by following the steps above from "Configuring the Delinea Add-on for Splunk" on the previous page
5. On the Splunk instance, configure receiving by navigating to **Settings** > **Forwarding and Receiving** > **Configure Receiving** > **New**. Enter the port on which events are forwarded (entered in step 2).

Linux

On a Linux machine, Delinea events are forwarded through syslog.

Follow these steps to configure syslog:

1. Enter the following information in **/etc/rsyslog.conf**:

   ```
   *.*@@\<IP-Address\>:\<port\>
   ```

   The **IP-address** should be the Splunk instance IP.
   The default port is 514.
2. Restart the rsyslog service using this command:

   Service rsyslog restart
3. On the Splunk instance, add data input to receive Delinea events:
   a. Go to: **Settings** > **Data Input** > **TCP** > **Add New** > Enter the port as in the **rsyslog.conf** file and select the source type as syslog.
   b. Click **Submit**.

Installation and Configuration for an On-Premise Deployment

This section describes the steps to:

- Install the Splunk Universal Forwarder
- Install the Delinea Add-on for Splunk
- Configure the Delinea Add-on for Splunk
- Install the Splunk Add-on for Windows
- Install the Splunk Add-on for Unix and Linux
- Forward data to the Indexer
- Install and configure Delinea Add-on for Splunk on the Indexer
- Install and configure Delinea Add-on and App for Splunk on the Search Head

Installing the Splunk Universal Forwarder

You must install the Splunk Universal Forwarder and one of the technology add-ons (TAs) such as Splunk Add-on for Windows/Unix and Linux or the Delinea Add-on for Splunk to collect Windows application logs. Follow the generic Splunk guidelines to install the Splunk Universal Forwarder on a Windows machine:

http://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Installtheuniversalforwardersoftware

Installing the Delinea Add-on for Splunk

Install the Splunk Universal Forwarder on a targeted system. If you are installing on the Splunk Universal Forwarder, the Splunk Web is not available.

You must extract the Add-on from the $SPLUNK_HOME/etc/apps directory.

Configuring the Delinea Add-on for Splunk for On-Premise Deployments

To configure the Delinea Add-on for Splunk for an on-premise deployment:

1. Make sure that you have admin rights to copy $SPLUNK_HOME/etc/apps/TA-centrify/default/inputs.conf.example
   to
   $SPLUNK_HOME/etc/apps/TA-centrify/local/inputs.conf

- There are different input stanzas in inputs.conf. This particular inputs.conf file contains entries for various file locations for monitoring syslog, depending on the OS platform.

2. To enable any stanza based on your OS, change the disabled property of the stanza from disabled=1 to disabled=0.
3. Note that source types are hard coded in the TA and you are advised not change this configuration.

- The reason for hard coding the source types is that Delinea dashboard apps are expecting very specific source types so if you change this practice, the dashboards stop working.
- Note: The index can be changed based on user needs.
- You can use the following configuration (example) when you want to index data with a specific index in $SPLUNK_HOME/etc/apps/TA-centrify/local/inputs.conf
- # Red Hat, CentOS, Citrix XenServer, oracle Enterprise Linux, Scientific Linux, Fedora, SUSE, openSUSE`

  [monitor:///var/log/messages] sourcetype = syslog

  disabled = 1

  index = centrify

4. Restart Splunk.

Installing the Splunk Add-on for Windows

Follow the generic Splunk guidelines to install the Splunk Add-on for Windows on a Windows machine:

https://docs.splunk.com/Documentation/WindowsAddOn/latest/User/InstalltheSplunkAdd-onforWindows

Installing the Splunk Add-on for Unix and Linux

Follow the generic Splunk guidelines to install the Splunk Add-on for Unix and Linux on a Unix machine:

http://docs.splunk.com/Documentation/UnixApp/latest/User/AbouttheSplunkAppforUnix

Forwarding Data to the Indexer

To forward data to the indexer:

1. Once you configure the Add-on, start forwarding data to the Indexer using the following command:

- $SPLUNK_HOME/bin/splunk add forward-server \<indexer\>:\<port\>
- Where is the Indexer's address and is the receiving port on the Indexer. Splunk recommends forwarding data on the Indexer port 9997.

2. See the list of configured Indexers using the outputs.conf file in: $SPLUNK_ HOME/etc/system/local/outputs.conf.

Indexers

To install the Delinea Add-on for Splunk (to install Splunk Enterprise on the Indexer):

1. Enable the receiving on the available port by going to: Splunk Web > Settings > Forwarding & Receiving > Configure Receiving and enable the port.

- Splunk recommends enabling receiving on port 9997.

2. Install the Delinea Add-on for Splunk on the Indexer.

- This step helps to index data in centrify_css_* sourcetype.

3. Restart Splunk.

To configure the Delinea Add-on for Splunk, you do not need to have a specific configuration for the Add-on.

If you are using an index other than the main one, create an index on the Indexer.

Search Heads

To install and configure Delinea Add-on and App for Splunk on the Search Head:

1. Install the Splunk Delinea Add-on for Splunk and the Delinea App for Splunk on your Search Heads.
2. To configure the Delinea App for Splunk, create an index in your default index list in Settings > Access Controls > Roles > (Click on a particular role) > Indexes Searched by default.

You do not need a special configuration for the Delinea Add-on for Splunk.

Note: The Forwarder, Indexer, and Search Head are on a single machine in a stand-alone deployment (but in a distributed environment, each component is on a separate machine).

Installation and Configuration for a Cloud Deployment

This section describes the steps to:

- Install the Splunk Universal Forwarder
- Install the Delinea Add-on for Splunk
- Configure the Delinea Add-on for Splunk

- Install the Splunk Add-on for Windows
- Install the Splunk Add-on for Unix and Linux
- Forward data to the Indexer
- Install and configure Delinea Add-on for Splunk on the Indexer
- Install and configure Delinea Add-on and App for Splunk on the Search Head

Installing the Splunk Universal Forwarder

You must install the Splunk Universal Forwarder and one of the technology add-ons (TAs) such as Splunk Add-on for Windows/Unix and Linux or the Delinea Add-on for Splunk to collect Windows application logs.

Follow the generic Splunk guidelines to install the Splunk Universal Forwarder on a Windows machine:

http://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Installtheuniversalforwardersoftware

Installing the Delinea Add-on for Splunk

To install the Splunk Universal Forwarder on a targeted system:

If you are installing on the Splunk Universal Forwarder, the Splunk Web is not available. Extract the Add-on from the $SPLUNK_HOME/etc/apps directory.

Configuring the Delinea Add-on for Splunk in cloud deployments

To configure the Delinea Add-on for Splunk in a cloud deployment:

1. Make sure that you have admin rights to copy $SPLUNK_HOME/etc/apps/TA-centrify/default/inputs.conf.example
   to
   $SPLUNK_HOME/etc/apps/TA-centrify/local/inputs.conf
   - There are different input stanzas in inputs.conf. This particular inputs.conf file contains entries for various file locations for monitoring syslog, depending on the OS platform.
2. To enable any stanza based on your OS, change the disabled property of the stanza from disabled=1 to disabled=0.
3. Note that source types are hard coded in the TA and you are advised not change this configuration.
   - The reason for hard coding the source types is that Delinea dashboard apps are expecting very specific source types so if you change this practice, the dashboards stop working.
   - Note: The index can be changed based on user needs.
   - You can use the following configuration (example) when you want to index data with a specific index in:
   - $SPLUNK_HOME/etc/apps/TA-centrify/local/inputs.conf

     Red Hat, CentOS, Citrix XenServer, oracle Enterprise Linux, Scientific Linux, Fedora, SUSE, openSUSE

     [monitor:///var/log/messages] sourcetype = syslog

     disabled = 1

index = centrify

4. Restart Splunk.

Installing the Splunk Add-on for Windows

Follow the generic Splunk guidelines to install the Splunk Add-on for Windows on a Windows machine:

https://docs.splunk.com/Documentation/WindowsAddOn/latest/User/InstalltheSplunkAdd-onforWindows

Installing the Splunk Add-on for Unix and Linux

Follow the generic Splunk guidelines to install the Splunk Add-on for Unix and Linux on a Unix machine:

http://docs.splunk.com/Documentation/UnixApp/latest/User/AbouttheSplunkAppforUnix

Forwarding Data to the Indexer

Follow these steps:

1. Once you configure the Add-on, start forwarding data to the Indexer using the following command: $SPLUNK_HOME/bin/splunk add forward-server__ <indexer>:<port>

- Where is the Indexer's address and is the receiving port on the Indexer. Splunk recommends forwarding data on the Indexer port 9997.

2. See the list of configured Indexers using the outputs.conf file in: $SPLUNK_ HOME/etc/system/local/outputs.conf.

Indexers

The procedure to install the Delinea Add-on for Splunk occurs in this manner:

You will have an open ticket with the Splunk Cloud team to install the Delinea Add-on on the Indexer. Installing the Delinea Add-on helps to index data in centrify_css_* sourcetype.

The Splunk cloud customers do not have direct access to their Indexers so they rely on the Splunk cloud team to do the configuration for them. The Splunk cloud team might create a separate index for them to ingest the data into a specific index. If this is the case, the inputs.conf file on the Universal Forwarder must be changed as described in Forwarding Data to the Indexer so that data is indexed properly.

To configure the Delinea Add-on for Splunk, you do not need to have a specific configuration for the Add-on.

Search Heads

You are expected to create a ticket with the Splunk cloud team to install the Splunk Delinea Add-on for Splunk and the Delinea App for Splunk on your Search Heads.

You do not need a special configuration for the Delinea Add-on for Splunk.

To configure the Delinea App for Splunk, an index created by the Splunk cloud team must be added in your default index list in:
Settings > Access Controls > Roles > (Click on a particular role) > Indexes Searched by default.

Note: The Forwarder, Indexer, and Search Head are on a single machine in a stand-alone deployment (but in a distributed environment, each component is on a separate machine).

Splunk Index and Source Types

Splunk indexes and source types are determined based on what method is used for data collection. You can either choose the existing installation of the Splunk Add-on for Windows and Unix and Linux or the Delinea Add-on for Splunk.

Data Collection Using the Splunk Add-on for Windows and Unix and Linux

In this scenario, data is indexed to **wineventlog**, and the OS indexes and source type is either the WinEventLog:Application(Windows) or the syslog (Unix). You must add these indexes to the default searchable indexes by going to:

Settings > **Access Controls** > **Roles** > (Click on a particular role) > **Indexes Searched** by default

Data Collection Using Delinea Add-on for Splunk

In this case, data is indexed to the main index and the source type is either **WinEventLog:Application**(Windows) or **syslog** (Unix). Delinea uses the same source types as the Splunk Add-on for Windows and Unix and Linux so that field extractions can be performed regardless of the data collection method that you choose.

This method also prevents your data from being replicated to multiple indexes regardless of the data collection method used, and ensures that the Delinea data is extracted correctly in all scenarios.

CIM Compliance

The Delinea Authentication events are mapped to the Authentication model of the CIM.

To search the Delinea authentication raw events, you can execute this search query:

Search tag=authentication app=Centrify

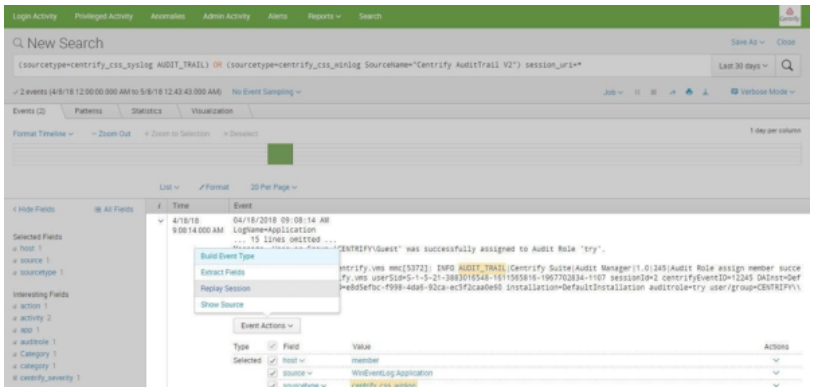
To search the Delinea failed or denied authentication data through a CIM authentication query, you can execute this search query:

```
| tstats values(Authentication.app) as app from datamodel=Authentication WHERE
Authentication.action=failure Authentication.app=Centrify by
Authentication.dest,Authentication.user,Authentication.action
```

Session Playback

Delinea records all privileged user activity including screen actions, events, and metadata, and delivers a comprehensive picture of intentions and impacts. Its unique, searchable playback feature gives IT security managers and auditors the ability to see exactly what users did and the results of their actions. Session playback identifies privilege abuse or the source of a security incident.

Delinea's session playback is externalized to Splunk with Delinea's Session Recording and Monitoring. You can now playback the session video from the Delinea Audit event as shown in the following example:



Verification

After the installation of the Delinea Add-on for Splunk is complete, all of the new Delinea audit trail events should be parsed and indexed by Splunk.

Sample Searches

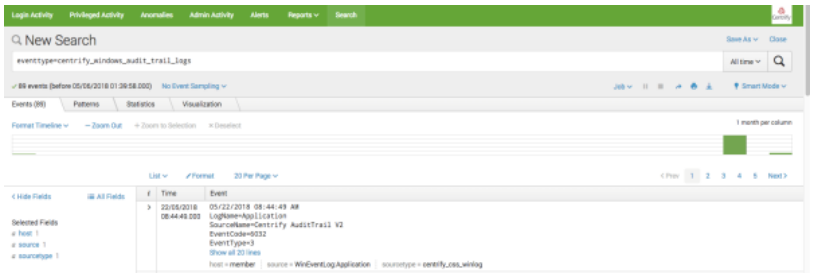
Use the following sample searches to validate your installation:

- Search all Delinea logs generated on Windows Agents:
  `Search eventtype=centrify_windows_audit_trail_logs`
- Search All Audit Analyzer-related logs:
  `Search eventtype=Centrify_audit_analyzer`
- Search all successful/granted DirectAuthorize-Windows logs:

  `Search eventtype=centrify_directauthorize_windows eventstatus=GRANTED`
- Search all failed/denied DirectAuthorize-Windows logs:

  `Search eventtype=centrify_directauthorize_windows eventstatus=DENIED`

The search results for all Delinea logs generated on Windows Agents is shown in the following example:



Troubleshooting

If data is not populating in the dashboards, try the following solutions to resolve the issue:

- The Delinea Add-On for Splunk should not be modified on the Universal Forwarder. Specifically, the source type should not be modified. Data should flow from either the **WinEventLog:Application or syslog**.

- The Delinea Add-On for Splunk should be installed on Indexers as it performs index time extraction and indexing data in respective source types. Data from the WinEventLog:Application source type will be indexed in the **centrify_css_winlog** and the syslog source type data will be indexed in the **centrify_css_syslog** source type.
- If a new index has been created, it should be updated in the default index list in the user Roles shown in following location:

  Settings > **Access Controls** > **Roles** > (Click on particular role) > Indexes Searched by default.

Privileged Access Service Developer Tasks

This section includes the following information about developer tools.

- "Importing Systems, Accounts, Domains, and Databases" on the next page
- "Exporting Privileged Access Service Data Using Escrow Functions" below
- "Assigning PowerShell Remote Access" below
- "Sample.csv Template Fields" on page 1195

Assigning PowerShell Remote Access

If you want to allow some of your users to be able to run PowerShell commands on remote computers by way of PowerShell remoting, be aware of the following requirements:

- The target computer needs to have the Delinea Client for Windows installed with the Privileged Access Service enabled.
- Assign the user to a role with the "PowerShell remote access is allowed" system right granted.

If you're using the Delinea Audit & Monitoring Service, when a user attempts to run PowerShell remotely on a computer, the system triggers an audit trail event. Delinea Audit & Monitoring Service is an optional service.

To assign PowerShell remote access to a user:

1. In the **Access Manager** console, open the zone that the Windows system to be managed belongs to (Access Manager is not necessarily installed on the machine with the Windows client).
2. Under **Role Definitions**, right-click a role that you'd like to assign PowerShell remote access permission to and select **Properties**.
3. Under **System Rights** > **Windows rights**, select **PowerShell remote access is allowed**.
4. Right-click **Role** > **Assignment** and select **Assign Role**.
5. Select the role as defined above and assign the Windows account to it.

Exporting Privileged Access Service Data Using Escrow Functions

Users with the System Administrator role can securely export encrypted data attributes including account passwords for Systems, Accounts, Domains, and Databases from Privileged Access Service using Delinea

commands and the Escrow PowerShell module. The data exported is aggregated into a CSV file, similar to the import Sample.csv template described in "Importing Systems, Accounts, Domains, Databases".

The exported data can be securely emailed to designated recipients using the PGP encryption program. If the amount of data before encryption and compression exceeds more than 20MB, the additional data is written to another file and sent to recipients in a second email. To open the email attachment that contains the data, you need to enter a passphrase to unlock the OpenPGP secret key.

Note: The data from the exported file can be imported back into Privileged Access Service (see "Importing Systems, Accounts, Domains, Databases".

Importing Systems, Accounts, Domains, and Databases

You can create an import file to add multiple entities (Systems, Accounts, Domains, and Databases) to Privileged Access Service, and their attributes using the import file template and the Delinea PowerShell script. The import file provides a comma-separated set of required and optional fields that describe the items you want to add. Once you populate the CSV file with the information you want imported into Privileged Access Service, you can run the Delinea PowerShell script and then access the content in the Admin Portal.

To download the import files and populate the CSV file:

1. Access Github at https://github.com/centrify/centrify-samples-powershell to download the import files to your local computer. The import files include the following:
   - Privileged Access Service PowerShell script (Centrify.Samples.PowerShell.Example.ps1)
   - You modify the script file to import entities and their attributes from the CSV file into Privileged Access Service.
     - Privileged Access Service PowerShell module file (Centrify.Sample.PowerShell.CPS.psm1)
   - The module file is called from the Delinea PowerShell script and does not require any modification.
     - CSV template (Sample.csv)
   - The import template illustrates the format to use in creating your own comma-separated values (CSV) file with all the entities and attributes you want to import.
2. Open the Sample.csv template in a text editor or spreadsheet program.
3. Click File, then Save As to save the file to a location on your local computer.
4. Edit your custom CSV file, using the template as a guideline, so that each line provides the information regarding Systems, Domains, Databases, and Accounts you want added to Privileged Access Service.
   - As illustrated by the examples in the template file, you can leave optional fields blank. When you are finished adding the entities you want to import, remove the template fields and examples—if you haven't done so already—and save your changes to the file.

For information on the available attributes and what they mean, see "Sample.csv template fields."

To import multiple systems, accounts, domains, and databases:

Verify that the computer you are using to import entities has access to the Privileged Access Service Admin Portal.

1. Open the Centrify.Samples.PowerShell.Example.ps1 script file you downloaded earlier and edit the param section of the script to include the following parameters for your instance:

- #[string]$username = "userexample@acme.com",
- #[string]$endpoint = "https://cloud.centrify.com",

2. Edit the Centrify.Samples.PowerShell.Example.ps1 to include a command like the following, where Endpointincludes your Privileged Access Service tenant and CSVFileincludes the path and name of the CSV file you created. For example:

- Centrify-CPS-Import -Endpoint 'https://cloud.centrify.com' -Token $token -CSVFile 'C:\ImportFile.csv'

3. Save the modified file and then start Windows PowerShell to open a command window.
4. Run the modified Centrify.Samples.PowerShell.Example.ps1 script by entering the full path to the script. For example, C:/scripts/Centrify.Samples.PowerShell.Example.ps1.

- The script calls theDelinea.Sample.PowerShell.CPS.psm1 module to import Systems, Domains, Databases, Accounts and their attributes into Privileged Access Service.
- Depending on the number of entities you are importing, the process might take some time to complete. Once complete, the script outputs the following files to a folder with information on the import status:
  - FailedRows.csv–this file includes all rows that failed to import into Privileged Access Service. You can fix the errors in this file and then re-import the content. If this file is not included in the output, the import was successful.
  - FailedRows.txt–this file provides a summary of the import result for failed rows.
  - WarningRows.txt–this file provides import results for the rows in the CSV file that imported with some errors and an explanation for the errors. If this file is empty, all content in the CSV file imported successfully. If the import fails to complete a particular operation, you can log in to the Admin Portal and correct the failed operation.
  - AllRows.txt–this file provides the results for all rows in the CSV file. The rows in this file are listed in the same order as the Sample.csv.

Sample.csv template fields

The following table describes the template fields in the Sample.csv file. Enter values for each entity type according to the headings designated in the template file. Do not change the template headings; the import functionality requires that the headings match those in the template exactly. The order that you enter entities (Systems, Domains, Databases, and Accounts) into the import file does not affect import functionality.

For this template field	You need to do this
Entity Type	Enter one of the following entity types:SystemDomainDatabaseAccountThis field is required.

For this template field	You need to do this
Name	Type the display name of the system, domain or database you want to add.As illustrated by the examples in the template, you can have multiple lines with the same name. For example, if you are adding more than one account for the same system, list each account as a separate line with the same system name. This field is required and applies to Systems, Domains, and Databases.
FQDN	Type the fully-qualified domain name or IP address of the System or Database you want to add. If you are only adding an account for a system that was previously added, you should not specify the FQDN field.This field is required and applies to Systems and Databases.
Description	Type any descriptive information you want to add for the entity. This field is optional and applies to Systems, Domains, Databases, and Accounts.
ComputerClass	Specify the type of system you are adding. You can specify one of the following values for this field:`WindowsUnixGenericSshCisco AsyncOSCiscoIOSCiscoNXOSJuniperJunosHPNonStopOSIBMiCheckPointGaiaPalo AltoNetworksPANOSF5NetworksBIGIPVMwareVMkernel`This field is required and applies to Systems.
ProxyUser	Type the name of the “proxy” user for a system. This field is optional and applies to Systems. For more information about the “proxy” user for Windows systems, see the following topic:"Configuring Proxy Users for Password Operations" on page 546 For more information about the “proxy” user for UNIX and Juniper systems, see the following topic:"Specifying Proxy Root Accounts" on page 537
ProxyUserPassword	Provide the password for the “proxy” user for a system. This field is optional and applies to Systems.
ProxyUserIsManaged	Specify whether you want to manage the password for the “proxy” user. This field is optional and applies to Systems. You can specify TRUE if you want the Privileged Access Service to manage the password for the “proxy” account, or FALSE if you want to leave the password unmanaged.
ResourceDomain	Type the name of the domain that the system is joined to. This field is optional and applies to Systems.
ResourceDomainOperationsEnabled	Specify whether you want to use the domain administrative account to enable zone role workflow. You specify TRUE if you want to use the domain administrative account to enable operations such as zone role workflow, or FALSE if you do not want to use the domain administrative account to enable domain operations. In order to enable domain operations for a system, the user must have grant rights over the domain or else the import will fail. This field is optional and applies to Systems.

For this template field	You need to do this
ResourceSessionType	Specify whether you want to use secure shell or remote desktop for remote connections. Enter Ssh for secure shell or Rdp for remote desktop. This field is required and applies to Systems.
ResourceSessionTypePort	Enter the port to be used for remote connections. You only need to enter a value if you do not want to use the default port (default port for SSH is 22 and for RDP it is 3389). This field is optional and applies to Systems.
ResourceWindowsManagementMode	For Windows System types , you can choose a management mode to manage the system.Enter one of the following management modes:Unknown (this is equivalent to auto-detect in the Admin Portal)SmbWinRMOverHttpWinRMOverHttpsRpcOverTcpDisabledThis field is optional and applies to Systems.
ResourceWindowsManagementPort	For Windows, F5 Networks BIG-IP, and Palo Alto Networks PAN-OS Systems, enter the management port to be used for password management. This field is optional and applies to Systems.
PasswordProfile	Enter a name to add a customized password profile to define the rules applied when managed passwords are generated for systems, domains, or databases. For more information about customizing a password profile, see "Configuring password profiles."This field is optional and applies to Systems, Domains, and Databases.
SetName	Enter a name for system, domain, database, or account sets. Sets are logical groups of a particular type (system, domain, database, or account) to simplify management activity and reporting for entities with attributes in common. To enter more than one set name for an entity, separate the entries by a |. For example, SystemSet1|SystemSet2|SystemSet3.This field is optional and applies to Systems, Domains, Databases, and Accounts.
DefaultCheckoutTime	Enter a number to specify the length of time (in minutes) that a checked out password is valid. The minimum checkout time is 15 minutes. If no value is specified, the default is 60 minutes. Also see Setting system-specific policies. This field is optional and applies to Systems, Domains, Databases, and Accounts.
AllowRemote	Enter TRUE if you want to allow remote connections from a public network for a selected system of FALSE if you do not want to allow remote connections from a public network.This field is optional and applies to Systems.
ParentEntityTypeOfAccount	Enter the type of entity related to the account (System, Domain or Database).This field is required and applies to Accounts.

For this template field	You need to do this
ParentEntityNameOfAccount	Enter the display name of the system, domain or database associated with the account. This field is required and applies to Accounts.
User	Type the user name for an account to be used with Systems, Domains, and Databases. This field is required and applies to Accounts.
Password	Type the password for the account to be used with the system.This field is optional and applies to Accounts.
IsManaged	Specify whether you want to manage the password for the user account you are adding for the system.You can specify TRUE if you want the Privileged Access Service to manage the password for the account, or FALSE if you want to leave the password unmanaged.This field is optional and applies to Accounts.
AccountMode	Enter the term Expert to add an expert mode account for Checkpoint Gaia systems. This field is optional and applies to Systems.
UseProxy	Specify whether you want to add a “proxy” account for the system.Specify TRUE if you want to use a “proxy” account, or FALSE if you don’t want to add a “proxy” account for the system.For UNIX and Juniper systems, use this field if your secure shell environment is configured to not allow the root user to access computers remotely using SSH. You can also use this field for Windows systems if you want to use a proxy account for Windows Remote Management (WinRM) connections to a system.This field is optional and applies to Accounts.
DatabaseServiceType	Specify the type of database you are adding.Enter one of the following types:SQLServerOracleSAP Adaptive Server Enterprise (ASE)This field is required and applies to Databases.
OracleServiceName	For Oracle databases, you must enter the service name assigned to the Oracle database. Also see "Adding Databases" on page 477. This field is required and applies to Databases.
SQLInstanceName	For SQL Server databases, you must enter the instance name assigned to the database. Also see "Adding Databases" on page 477. This field is optional and applies to Databases.
DatabasePort	Specify the port number used to check the status of the database and when updating database passwords. This field is optional and applies to Databases.
ParentDomain	If a child domain is configured, enter the name of its parent domain.This field is optional and applies to Domains.

For this template field	You need to do this
AdministrativeAccount	Enter an account in the format admin@childdomain, admin@mycompany.com or a local account that needs to be set as the administrative account.This field is optional and applies to Systems and Domains.
AllowAutomaticAccountMaintenance	Specify TRUE to allow out-of-sync passwords to be reset and managed accounts to be unlocked during login or checkout, or FALSE if you do not want to allow it. Requires an Administrative Account be defined for the domain.This field is optional and applies to Domains.
AllowManualAccountUnlock	Specify TRUE to allow users with the Unlock Account permission to manually unlock accounts, or FALSE if you do not want to allow accounts to be manually unlocked. Requires an Administrative Account be defined for the domain.This field is optional and applies to Domains.
AllowMultipleCheckouts	Specify whether multiple users can have the same domain account password checked out at the same time for a system, domain, or database.Enter FALSE if only one user is allowed to check out the password at any given time. Enter TRUE if you want to allow multiple users to have the account password checked out at the same time without waiting for the password to be checked in. Also see, Allow multiple password checkouts. This field is optional and applies to Systems, Domains, and Databases.
AllowPasswordRotation	Specifies if the managed password should be rotated periodically by Privileged Access Service for a system, domain, or database.Enter TRUE to allow periodic password rotation or FALSE to not allow periodic password rotation.This field is optional and applies to Systems, Domains, and Databases.
PasswordRotateDuration	Specifies the interval at which managed passwords are automatically rotated.Enter the maximum number of days to allow between automated password changes for managed system, domain, or database accounts.This field is optional and applies to Systems, Domains, and Databases.
MinimumPasswordAge	Enter the minimum number of days before a password must be rotated.This field is optional and applies to Systems, Domains, and Databases.
AllowPasswordHistoryCleanUp	Specifies if the retired passwords should be deleted periodically by Privileged Access Service.Enter TRUE to allow periodic password history cleanupor FALSE to not allow periodic password history cleanup.This field is optional and applies to Systems, Domains, and Databases.
PasswordHistoryCleanUpDuration	Enter the number of days after which retired passwords matching the duration are deleted.This field is optional and applies to Systems, Domains, and Databases.

Sample.csv Template Fields

The following table describes the template fields in the Sample.csv file. Enter values for each entity type according to the headings designated in the template file. Do not change the template headings; the import functionality requires that the headings match those in the template exactly. The order that you enter entities (Systems, Domains, Databases, and Accounts) into the import file does not affect import functionality.

For this template field	You need to do this
Entity Type	Enter one of the following entity types: System Domain Database Account This field is required.
Name	Type the display name of the system, domain or database you want to add. As illustrated by the examples in the template, you can have multiple lines with the same name. For example, if you are adding more than one account for the same system, list each account as a separate line with the same system name. This field is required and applies to Systems, Domains, and Databases.
FQDN	Type the fully-qualified domain name or IP address of the System or Database you want to add. If you are only adding an account for a system that was previously added, you should not specify the FQDN field. This field is required and applies to Systems and Databases.
Description	Type any descriptive information you want to add for the entity. This field is optional and applies to Systems, Domains, Databases, and Accounts.
ComputerClass	Specify the type of system you are adding. You can specify one of the following values for this field: Windows Unix GenericSsh Cisco AsyncOS CiscoIOS CiscoNXOS JuniperJunos HPNonStopOS IBMi CheckPointGaia PaloAltoNetworksPANOS F5NetworksBIGIP VMwareVMkernel This field is required and applies to Systems.
ProxyUser	Type the name of the “proxy” user for a system. This field is optional and applies to Systems. For more information about the “proxy” user for Windows systems, see the following topic: Configuring a proxy user for password operations For more information about the “proxy” user for UNIX and Juniper systems, see the following topic: Specifying a proxy account for root

For this template field	You need to do this
ProxyUserPassword	Provide the password for the “proxy” user for a system. This field is optional and applies to Systems. For more information about the “proxy” user for Windows systems, see the following topic: Configuring a proxy user for password operations For more information about the “proxy” user for UNIX and Juniper systems, see the following topic: Specifying a proxy account for root
ProxyUserIsManaged	Specify whether you want to manage the password for the “proxy” user. This field is optional and applies to Systems. You can specify TRUE if you want the Privileged Access Service to manage the password for the “proxy” account, or FALSE if you want to leave the password unmanaged.
ResourceDomain	Type the name of the domain that the system is joined to. This field is optional and applies to Systems.
ResourceDomainOperationsEnabled	Specify whether you want to use the domain administrative account to enable zone role workflow. You specify TRUE if you want to use the domain administrative account to enable operations such as zone role workflow, or FALSE if you do not want to use the domain administrative account to enable domain operations. In order to enable domain operations for a system, the user must have grant rights over the domain or else the import will fail. This field is optional and applies to Systems.
ResourceSessionType	Specify whether you want to use secure shell or remote desktop for remote connections. Enter Ssh for secure shell or Rdp for remote desktop. This field is required and applies to Systems.
ResourceSessionTypePort	Enter the port to be used for remote connections. You only need to enter a value if you do not want to use the default port (default port for SSH is 22 and for RDP it is 3389). This field is optional and applies to Systems.
ResourceWindowsManagementMode	For Windows System types , you can choose a management mode to manage the system. Enter one of the following management modes: Unknown (this is equivalent to auto-detect in the Admin Portal) Smb WinRMOverHttp WinRMOverHttps RpcOverTcp Disabled This field is optional and applies to Systems.
ResourceWindowsManagementPort	For Windows, F5 Networks BIG-IP, and Palo Alto Networks PAN-OS Systems, enter the management port to be used for password management. This field is optional and applies to Systems.

For this template field	You need to do this
PasswordProfile	Enter a name to add a customized password profile to define the rules applied when managed passwords are generated for systems, domains, or databases. For more information about customizing a password profile, see Configuring password profiles. This field is optional and applies to Systems, Domains, and Databases.
SetName	Enter a name for system, domain, database, or account sets. Sets are logical groups of a particular type (system, domain, database, or account) to simplify management activity and reporting for entities with attributes in common. To enter more than one set name for an entity, separate the entries by a |. For example, SystemSet1|SystemSet2|SystemSet3. This field is optional and applies to Systems, Domains, Databases, and Accounts.
DefaultCheckoutTime	Enter a number to specify the length of time (in minutes) that a checked out password is valid. The minimum checkout time is 15 minutes. If no value is specified, the default is 60 minutes. Also see, Setting systemspecific policies. This field is optional and applies to Systems, Domains, Databases, and Accounts.
AllowRemote	Enter TRUE if you want to allow remote connections from a public network for a selected system of FALSE if you do not want to allow remote connections from a public network. This field is optional and applies to Systems.
ParentEntityTypeOfAccount	Enter the type of entity related to the account (System, Domain or Database). This field is required and applies to Accounts.
ParentEntityNameOfAccount	Enter the display name of the system, domain or database associated with the account. This field is required and applies to Accounts.
User	Type the user name for an account to be used with Systems, Domains, and Databases. This field is required and applies to Accounts.
Password	Type the password for the account to be used with the system. This field is optional and applies to Accounts.
IsManaged	Specify whether you want to manage the password for the user account you are adding for the system. You can specify TRUE if you want the Privileged Access Service to manage the password for the account, or FALSE if you want to leave the password unmanaged. This field is optional and applies to Accounts.

For this template field	You need to do this
AccountMode	Enter the term Expert to add an expert mode account for Checkpoint Gaia systems. This field is optional and applies to Systems.
UseProxy	Specify whether you want to add a “proxy” account for the system. Specify TRUE if you want to use a “proxy” account, or FALSE if you don’t want to add a “proxy” account for the system. For UNIX and Juniper systems, use this field if your secure shell environment is configured to not allow the root user to access computers remotely using SSH. You can also use this field for Windows systems if you want to use a proxy account for Windows Remote Management (WinRM) connections to a system. This field is optional and applies to Accounts.
DatabaseServiceType	Specify the type of database you are adding. Enter one of the following types: SQLServer Oracle SAP Adaptive Server Enterprise (ASE) This field is required and applies to Databases.
OracleServiceName	For Oracle databases, you must enter the service name assigned to the Oracle database. Also see, Adding databases. This field is required and applies to Databases.
SQLInstanceName	For SQL Server databases, you must enter the instance name assigned to the database. Also see, Adding databases. This field is optional and applies to Databases.
DatabasePort	Specify the port number used to check the status of the database and when updating database passwords. This field is optional and applies to Databases.
ParentDomain	If a child domain is configured, enter the name of its parent domain. This field is optional and applies to Domains.
AdministrativeAccount	Enter an account in the format admin@childdomain, admin@mycompany.com or a local account that needs to be set as the administrative account. This field is optional and applies to Systems and Domains.
AllowAutomaticAccountMaintenance	Specify TRUE to allow out-of-sync passwords to be reset and managed accounts to be unlocked during login or checkout, or FALSE if you do not want to allow it. Requires an Administrative Account be defined for the domain. This field is optional and applies to Domains.

For this template field	You need to do this
AllowManualAccountUnlock	Specify TRUE to allow users with the Unlock Account permission to manually unlock accounts, or FALSE if you do not want to allow accounts to be manually unlocked. Requires an Administrative Account be defined for the domain. This field is optional and applies to Domains.
AllowMultipleCheckouts	Specify whether multiple users can have the same domain account password checked out at the same time for a system, domain, or database. Enter FALSE if only one user is allowed to check out the password at any given time. Enter TRUE if you want to allow multiple users to have the account password checked out at the same time without waiting for the password to be checked in. Also see, Allow multiple password checkouts. This field is optional and applies to Systems, Domains, and Databases.
AllowPasswordRotation	Specifies if the managed password should be rotated periodically by Privileged Access Service for a system, domain, or database. Enter TRUE to allow periodic password rotation or FALSE to not allow periodic password rotation. This field is optional and applies to Systems, Domains, and Databases.
PasswordRotateDuration	Specifies the interval at which managed passwords are automatically rotated. Enter the maximum number of days to allow between automated password changes for managed system, domain, or database accounts. This field is optional and applies to Systems, Domains, and Databases.
MinimumPasswordAge	Enter the minimum number of days before a password must be rotated. This field is optional and applies to Systems, Domains, and Databases.
AllowPasswordHistoryCleanUp	Specifies if the retired passwords should be deleted periodically by Privileged Access Service. Enter TRUE to allow periodic password history cleanupor FALSE to not allow periodic password history cleanup. This field is optional and applies to Systems, Domains, and Databases.
PasswordHistoryCleanUpDuration	

PAS and Cloud Suite Release Notes

Follow the links below to go to Cloud Suite and PAS release notes.

Cloud Suite - Release Notes

Be sure to read the "Privileged Access Service - Release Notes" on page 1210 also.

23.1 Release Notes

This update includes the following features, updates, and other changes. These release notes cover information specific to Cloud Suite and Privileged Access Service.

Note: After applying the February, 14, 2023, Microsoft Update KB5022842 (OS Build 20348.1547) on a Virtualized Windows Server 2022 with Secure Boot Enabled server will become unusable. This issue is reproducible **without** any Delinea products installed on the Windows Server 2022 system.

Cause: The issue arises on the second reboot after installing the Microsoft update KB5022842 on Windows Server 2022 that is running on VMWare vSphere ESXi 6.7 U2/U3 or vSphere ESXi 7.0.x. Delinea recommends the best practice is to create system restore points prior to doing any upgrades, patches or system changes.

New Features

Granular Privilege Elevation Workflow UI

- This enables users to submit workflow requests with specific Privilege Elevation commands.
- Users can find a system in PAS, request Privilege Elevation permission, and then select specific commands or command sets as set up by the administrator.

Documentation

You can find the documentation under the following sections:

Notice of Discontinuation

None.

Resolved Issues and Changes in 23.1

- Fixed the email authentication issues. When users select email as an option to authenticate to PAS, the user won't be seeing a URL link to authenticate in the email which the user has received. The user will have to manually enter the One Time Passcode where the user has initiated the login session. (ref: 469681)
- Fixed the ability to log in or rotate passwords for AWS Cloud Provider Root Account. (ref:461023)
- Fixed account password rotation for Multiplexed Accounts. Users with edit, delete and grant permissions for the Multiplex Account will automatically have view permission for such accounts. (ref:463715)
- Fixed an issue when emailing reports of "HTML Table" export type with report parameters of integer type would fail. (ref:466537)
- HTML requests to reports data provider RedRock endpoint are protected with the user's role report management. (ref:468164)
- Fixed IOS enrollment issues affecting some tenants who were unable to enroll on the IOS mobile app. (ref:470660)
- Fixed adding command sets to Global Privilege Elevation. Users will now be able to add command sets. (ref:474752)
- Fixed Privilege Elevation addition wizard for enrolled system second step. The add button is enabled only when 'user', 'group', or 'role' is chosen. (ref:474862)
- Errors in the workflow process were corrected, allowing access to secrets. (ref:464006)

Resolved Issues and Changes in 23.1 HF11

- Enhanced access and retrieval times for secrets and folders in the PAS portal UI and API, allowing users to access them faster. (ref: 575357)

Resolved Issues and Changes in 23.1 HF9

- Fixed an issue where the system failed to account for Cisco SSH templates using a 'host' field instead of the typical 'machine' or 'domain' fields found in other UNIX SSH templates. (ref: 478014)
- Improved security around OTP Code verification. (ref: 578891)

Resolved Issues and Changes in 23.1 HF7

- Fixed a security issue where directory listing information was not properly restricted via an API endpoint. (ref: 551074)
- Fixed a security issue where unrestricted file download was possible through an API. (ref: 551072)

Clients for Linux

Added support for Rocky Linux and Alma Linux:

- Rocky Linux 8.6
- Alma Linux 8.6

Clients for Microsoft Windows

- Cloud Client is allowed to be installed with all features enabled on Windows Workstations so that customers may log in with cloud brokered identities and perform MFA at login.
- Customers will also be able to perform tasks based on DMC and AAPM features.

Known Issues

- When adding specific commands or command sets to a Privilege Elevation Command workflow, you must type the Privilege Elevation commands or command sets names in the search bar so that you can select them. Commands or sets will not automatically show up to be selected.
- If you currently have Privilege Elevation commands or sets assigned to a system, the Request Privilege Elevation option will not show up under the Actions menu for the system.

Client Known Issues

- When you log in to an enrolled system and your account is set up to use MFA redirection, the service prompts you for your password, not the password for the MFA redirect user. This feature is available on systems that have the Cloud Client installed and enrolled.

MFA Known Issues

- Ensure that required data for each selected authentication factor is present when selecting the use of a secondary factor (SMS, phone, email, etc). You should ensure that the data is present in Active Directory for all users otherwise it is possible that users with missing data may be locked out. You can specify a preferred factor and if not present an alternative factor will be used. For example, if a user has no phone number in AD and SMS was the preferred factor, the Delinea PAS will fall back to another selected factor (for example, email). If there is no phone number or email in AD in this case, the user would be locked out.
- Email as an MFA mechanism is subject to spam or junk filters. Be aware that using email as an MFA mechanism may be affected by users' email providers' spam or junk filters.
- SMS or phone are only attempted once a password is validated. This prevents spam and billing issues if an attacker attempts to brute force passwords to gain entry.
- For FIDO2 and On-Device Authentication options you will need to log in from the tenant specific URL.

22.3 Release Notes

This update includes the following features, fixes, and other changes. These release notes cover information specific to Cloud Suite; be sure to read the "22.3 Release Notes" on page 1213.

> After applying the February/14/2023, Microsoft Update KB5022842 (OS Build 20348.1547) on a Virtualized Windows Server 2022 with Secure Boot Enabled server will become unusable. This issue is reproducible **without** any Delinea products installed on the Windows Server 2022 system.

Cause: The issue arises on the second reboot after installing the Microsoft update KB5022842 on Windows Server 2022 that is running on VMWare vSphere ESXi 6.7 U2/U3 or vSphere ESXi 7.0.x. Delinea recommends the best practice is to create system restore points prior to doing any upgrades, patches or system changes.

New Features

Privilege Elevation with added group privileges (Windows)

- This enables users to run Elevated Privilege commands with the same user that is connected to the session with added local Administrator group privileges as opposed to running the command with a local `<username>-priv` user created just for this purpose.

Set-Based Unix Profile Role Mapping Settings

- This enables customers to expose PAS Roles as sets of enrolled Linux systems as compared to exposing such roles on all enrolled systems (which is the current behavior).

Granular Privilege Elevation Workflow Preview

- This enables users in the command line to request Privilege Elevation privileges to specific commands or command sets as compared to always requesting privileges to run ALL commands as Administrator/root.
- When adding a new Privilege Elevation command the users can add a local user to run any privilege command. The user has to append the **Run As User** field with **@localhost** (example: localuser@localhost).

Documentation

You can find the documentation at the under the following sections:

- "Cloud Suite - Release Notes" on page 1200
- "Privileged Access Service - Release Notes" on page 1210

Notice of Discontinuation

None.

Resolved Issues and Changes in 22.3

- Cloud Suite features such as AgentAuth, AAPM, and DMC are now supported on Windows Workstations (Windows 10 and 11).
- Fixed an issue related to privilege elevation workflow activity, where the events in the Activity log showed that commands were run without an authentication challenge when in fact the user was challenged with additional authentication requests when they ran the command after the workflow request was approved. (ref:388576)
- Fixed an issue where if you use the `cenroll` command with just the `-z` option and no argument attached to it, that command combination now throws an appropriate error. (ref:448531)
- When a user selects **Email** as an option to authenticate to PAS, the user won't see a URL link to authenticate in the email sent to the user. The user will need to manually enter the **One Time Passcode** where the user has initiated the login session.

Resolved Issues and Changes in 22.3 HF1

- Support for additional ARN formats are now supported when managing AWS credentials. (ref:416069)
- Improved WebRDP experience related to network latency. (ref:431794)

Supported Platforms

Clients for Linux

Added support for Rocky Linux and Alma Linux:

- Rocky Linux 8.6
- Alma Linux 8.6

Clients for Microsoft Windows

- The Cloud Suite agent allowed to be installed with all features enabled on Windows Workstations so that customers may log in with cloud brokered identities and perform MFA at login.
- Customers will also be able to perform tasks based on DMC and AAPM features.

Known Issues

Client Known Issues

- When you log in to an enrolled system and your account is set up to use MFA redirection, the service prompts you for your password, not the password for the MFA redirect user. This feature is available on systems that have the Cloud Client installed and enrolled.

MFA Known Issues

- Ensure required data for each selected authentication factor is present When selecting the use of a secondary factor (SMS, phone, email, etc) you should ensure that the data is present in Active Directory for all users otherwise it is possible that users with missing data may be locked out. You can specify a preferred factor and if not present an alternative factor will be used. For example, if a user has no phone number in AD and SMS was the preferred factor, the Delinea PAS will fall back to another selected factor (for example, email). If there is no phone number or email in AD in this case, the user would effectively be locked out.
- Email as an MFA mechanism is subject to spam / junk filters Be aware that using email as an MFA mechanism may be affected by users' email providers' spam or junk filters.
- SMS / phone are only attempted once a password is validated This prevents spam and billing issues if an attacker attempts to brute force passwords to gain entry.
- For FIDO2 and On-Device Authentication options you will need to login from the tenant specific URL .

22.2 Release Notes

This update includes the following features, fixes, and other changes. These release notes cover information specific to Cloud Suite; be sure to read the "22.2 Release Notes" on page 1215 too.

New Features

Delinea and Centrify

We have updated the look and feel of the Cloud Client installer to reflect the new Delinea logo and colors. All files, folders, directories, settings, and registry keys and so forth remain as Centrify, as does the Admin Portal for PAS.

For more information about Delinea, see Delinea Announcement

Documentation

You can find the documentation under the following sections:

- "Cloud Suite - Release Notes" on page 1200
- "Privileged Access Service - Release Notes" on page 1210

Notice of Discontinuation

None

Resolved Issues and Changes in 22.2

Here are the resolved issues and behavior changes in this release:

- Added a new API `SetFeatureState` to update the state of a feature on an enrolled system. Only a sysadmin can call this API. In a single call, multiple features of a single enrolled system can be enabled/disabled. You can find more information about APIs at ourDeveloper Portal.
- Changed Privilege Elevation Commands to update the Display Name when the Name was changed.

Resolved Issues and Changes in 22.2 HF 1

- Fixed an issue with the Privilege Elevation Command screen where the page wouldn't load after clicking the Add button.

Supported Platforms

Be sure to read the "22.2 Release Notes" on page 1215 for more supported platforms for the Connector and so forth.

Clients for Linux

Client for Red Hat

- Red Hat Enterprise Linux 7.9, 8.3
- CentOS 7.9, 8.3
- Fedora 33, 34
- Oracle Linux 7.9, 8.3
- Amazon Linux 2 Latest Version

Client for Red Hat (ARM architecture):

- 7.9, 8.3

Client for SUSE

- SUSE15-SP3

Client for Debian

- Debian 9.13, 10.9, 11.2
- Ubuntu 18.04LTS, 20.04LTS, 21.04

Client for Alpine Linux

- Alpine Linux 3.14

> Before you uninstall the Cloud Client for Linux from an Alpine Linux system, you must unenroll the system first. The Alpine Linux package manager doesn't allow the service to verify that the client is unenrolled from Delinea PAS before uninstalling. If you uninstall the client without unenrolling first, you won't be able to log in to the system anymore.

Clients for Microsoft Windows

Windows 10 LTSB/LTSC, Windows Server 2012r2, 2016, 2019 LTSC, Windows 2022

Known Issues

Client Known Issues

- When you log in to an enrolled system and your account is set up to use MFA redirection, the service prompts you for your password, not the password for the MFA redirect user. This feature is available on systems that have the Cloud Client installed and enrolled.
- For privilege elevation workflow activity, the events in the Activity log show that commands were run without an authentication challenge when in fact the user was challenged with additional authentication requests when running the command after the workflow request is approved.

MFA Known Issues

- Ensure required data for each selected authentication factor is present When selecting the use of a secondary factor (SMS, phone, email, etc) you should ensure that the data is present in Active Directory for all users otherwise it is possible that users with missing data may be locked out. You can specify a preferred factor and if not present an alternative factor will be used. For example, if a user has no phone number in AD and SMS was the preferred factor, the Delinea PAS will fall back to another selected factor (for example, email). If there is no phone number or email in AD in this case, the user would effectively be locked out.
- Email as an MFA mechanism is subject to spam / junk filters Be aware that using email as an MFA mechanism may be affected by users' email providers' spam or junk filters.
- SMS / phone are only attempted once a password is validated This prevents spam and billing issues if an attacker attempts to brute force passwords to gain entry.
- For FIDO2 and On-Device Authentication options you will need to login from the tenant specific URL .

22.1 Release Notes

This update includes the following features, fixes, and other changes.

New Features

Ability to Deploy user.ignore and group.ignore Files to Multiple Systems

You can deploy the user.ignore and group.ignore configuration files to one or more enrolled Linux systems. You can deploy these files to individual systems or all systems in a set, and to no more than 500 systems at a time.

For details, see "Deploying the user.ignore and group.ignore Configuration Files" on page 688.

More Support for Local Linux Group Mapping

You can now map roles in Privileged Access Service to either new or existing Linux local groups. Previously you could map roles to just new local groups.

For details, see "Specifying UNIX Profile Information" on page 231.

Cloud Client Automatic Update Activity

When the Cloud Client attempts to do an automatic update, it will send the auto-update results to the target system's Activity tab. This will be available when the current version of the client (22.1) is automatically updated to a newer version.

Notice of Discontinuation

None

Resolved Issues and Changes

Here are the resolved issues and behavior changes in this release:

- Fixed an issue where in some cases the connector would not automatically restart after automatically upgrading to a new version.
- Fixed the issue where if you tried to elevate privileges for a user whose account name has 16 or more characters in it, privilege elevation failed with an error.
- Fixed an issue that might cause heavy database CPU usage intermittently.
- Fixed an issue where a user was prompted for user credentials twice when logging in to a system remotely using the "Enter Account" action.
- Fixed an issue that caused inconsistent Dark Mode behavior.
- Fixed an issue where running the report “User MFA Challenge Setup Status” might result in a query error.
- Fixed an issue where “Bulk Delete” might not delete some service accounts.
- Fixed an issue where the service didn't send Radius configuration information on connector startup.
- There are new reports related to privilege elevation activities; you can find these reports in the Resource Reports group.
- Fixed an issue where, under certain circumstances, if you tried to reset your password in the PAS Admin Portal by way of the Forgot Password option and there were multiple authentication challenges set up, the second required authentication challenge immediately skipped to the next step and failed.

Supported Platforms

Delinea Connector

- Windows Server 2012r2, Server 2016, Server 2019

Hyper-scalable Delinea Privileged Access Service

- Windows Server 2016, Server 2019, Windows Server 2022

Clients for Linux

Client for Red Hat

- Red Hat Enterprise Linux 7.9, 8.3
- CentOS 7.9, 8.3
- Fedora 33, 34
- Oracle Linux 7.9, 8.3
- Amazon Linux 2 Latest Version

Client for Red Hat (ARM architecture):

- 7.9, 8.3

Client for SUSE

- SUSE15-SP3

Client for Debian

- Debian 9.13, 10.9, 11.2
- Ubuntu 18.04LTS, 20.04LTS, 21.04

Client for Alpine Linux

- Alpine Linux 3.14

> Before you uninstall the Delinea Client for Linux from an Alpine Linux system, you must unenroll the system first. The Alpine Linux package manager doesn't allow the service to verify that the client is unenrolled from Delinea PAS before uninstalling. If you uninstall the client without unenrolling first, you won't be able to log in to the system anymore.

Clients for Microsoft Windows

Windows 10 LTSB/LTSC, Windows Server 2012r2, 2016, 2019 LTSC, Windows 2022

Windows PAS Remote Access Kit

Windows 10, Server 2012r2, Server 2016, Server 2019

Centrify App for Android

Android 5 (API level 21) and later

Centrify App for iOS

iOS 12 and above

Databases

- Microsoft SQL Server (versions 2008R2 and later)
- Oracle (versions 11.2.0.4, 12.1.0.1, 12.1.0.2)
- SAP ASE (version 16.0)

Network Devices and Appliances

- Check Point Gaia (versions R77.30, R80.10)
- Cisco AsyncOS (versions v10 and v11)
- Cisco IOS (versions IOS 12.1/IOS 15.0)
- Cisco NX-OS (version NX-OS 6.0)
- F5 Networks BIG-IP (versions v11, v12, v13)
- HP Nonstop OS (J06.19, H06.29)
- IBM i (versions IBM i 7.2, IBM i 7.3)
- Juniper Junos OS (version JunOS 12.3R6.6)
- Palo Alto Networks PAN-OS (versions 7.1, 8.0)
- VMware VMkernel (versions 5.5, 6.0, 6.5 and 6.7)
- Generic SSH

Desktop Apps

Privileged Access Service provides templates for the following Windows applications in the Desktop Apps feature. Privileged Access Service supports any versions of these applications that are compliant with the requirements for Windows Server 2012 R2 / 2016 Remote Desktop Services and RemoteApp. These applications must accept and process the command line strings pre-defined within the Desktop Apps templates. We have officially tested the following versions:

- SQL Server Management Studio (versions 13.0.15600.2, 2016 and 12.0.4522.0, 2012)
- TOAD for Oracle (version 13.0.0.80)
- VMware vSphere Client (version 6.0.0)

VMware vSphere Client supports VMware VMkernel systems with a VMkernel system version below 6.5

Custom user-defined templates are also available for additional desktop applications.

Known Issues

Client Known Issues

- When you log in to an enrolled system and your account is set up to use MFA redirection, the service prompts you for your password, not the password for the MFA redirect user. This feature is available on systems that have the Delinea Client installed and enrolled.
- For privilege elevation workflow activity, the events in the Activity log show that commands were run without an authentication challenge when in fact the user was challenged with additional authentication requests when running the command after the workflow request is approved.

MFA Known Issues

- Ensure required data for each selected authentication factor is present When selecting the use of a secondary factor (SMS, phone, email, etc) you should ensure that the data is present in Active Directory for all users otherwise it is possible that users with missing data may be locked out. You can specify a preferred factor and if not present an alternative factor will be used. For example, if a user has no phone number in AD and SMS was the preferred factor, the Delinea PAS will fall back to another selected factor (for example, email). If there is no phone number or email in AD in this case, the user would effectively be locked out.
- Email as an MFA mechanism is subject to spam / junk filters Be aware that using email as an MFA mechanism may be affected by users' email providers' spam or junk filters.
- SMS / phone are only attempted once a password is validated This prevents spam and billing issues if an attacker attempts to brute force passwords to gain entry.
- For FIDO2 and On-Device Authentication options you will need to login from the tenant specific URL .

Privileged Access Service - Release Notes

If you use Cloud Suite, be sure to read the "Cloud Suite - Release Notes" on page 1200 also.

23.1.2 HSPAS Release Notes

This update includes the following features, updates, and other changes. These release notes cover information specific to Privileged Access Service.

New Features

Logging Enhancements for 23.1.2

- This update includes log entries for API events including any updates to the following:
  - Roles
  - Systems
  - Settings
  - Tenant configurations regarding IP addresses
  - Logins
  - Privilege elevations
  - Machine resources.
- Additional details have been integrated to log events when PE commands are deleted or edited, permissions are removed or added, systems are added or removed from a set, and when adding users to a portal.

Resolved Issues and Changes in HSPAS 23.1.2

- Fixed an error with Cloud Suite Agent login where redirect users failed when 'Authenticate Profile' was set to 'Password + Mobile Auth'. (ref: 459211)
- Fixed an error when the Web RDP to Windows System had the RDP settings 'Window Size' set to 'Full Screen', and scroll bars on the bottom right of the Web RDP session screen appeared. (ref: 512725)
- Fixed an error where Alma Linux Cloud Suite Agents were not able to report their proper version and automatically upgrade. (ref: 518314)
- Fixed an error where the DynamicInvoker would fail on a AWS hosted tenant when red rock queries were invoked for specific function calls due to additional required parameters. (ref: 525097)
- Fixed a Privilege Elevation command failure where only one RunAs User was listed. (ref: 527216)
- Cloud SuiteTenant has guardrails in place to prevent the execution of queries that return large result sets when gathering data from the events table. These queries are used when generating specific types of reports. During the execution of the reports, large query results may cause excessive strain on resources and impact the performance at both tenant and pod levels. An error in the source code was identified, which allows the system to ignore the existing guardrails and return results of any size. The update will enforce the guardrails and prevent excessively large queries during report generation, minimizing the impact on the Cloud SuiteCloud Suite Tenant's performance. (ref: 535762)
- HSPAS now supports PostgreSQL 14 and 15. PostgreSQL 14 only supports SQL mode. Removed PostgreSQL version 11 because PostgreSQL no longer supports it. (ref: 536212, 564747)
- Fixed the email authentication issues. When users select email as an option to authenticate to PAS, the user won't be seeing a URL link to authenticate in the email which the user has received. The user will have to manually enter the One Time Passcode where the user has initiated the login session. (ref: 469681)
- Fixed the ability to log in or rotate passwords for AWS Cloud Provider Root Account. (ref:461023)

- Fixed account password rotation for Multiplexed Accounts. Users with edit, delete and grant permissions for the Multiplex Account will automatically have view permission for such accounts. (ref:463715)
- Fixed an issue when emailing reports of "HTML Table" export type with report parameters of integer type would fail. (ref:466537)
- HTML requests to reports data provider RedRock endpoint are protected with the user's role report management. (ref:468164)
- Fixed IOS enrollment issues affecting some tenants who were unable to enroll on the IOS mobile app. (ref:470660)
- Fixed adding command sets to Global Privilege Elevation. Users will now be able to add command sets. (ref:474752)
- Fixed Privilege Elevation addition wizard for enrolled system second step. The add button is enabled only when 'user', 'group', or 'role' is chosen. (ref:474862)
- Errors in the workflow process were corrected, allowing access to secrets. (ref:464006)

Resolved Issues and Changes in 23.1 HF9

- Fixed an issue where the system failed to account for Cisco SSH templates using a 'host' field instead of the typical 'machine' or 'domain' fields found in other UNIX SSH templates. (ref: 478014)
- Improved security around OTP Code verification. (ref: 578891)

Resolved Issues and Changes in 23.1 HF8

- Added support for PostgreSQL 15 on RHEL 9.2 with HSPAS.
- Discontinued support for PLV8 on HSPAS. Users should switch to using FastSQL instead. Before data migration, make sure that all PLV8 extensions are dropped.

Resolved Issues and Changes in 23.1 HF7

- Fixed a security issue where directory listing information was not properly restricted via an API endpoint. (ref: 551074)
- Fixed a security issue where unrestricted file download was possible through an API. (ref: 551072)

Known Issues

MFA Known Issues

- CBE functions are not working in the Firefox browser. When trying to log in as an AWS root user in the Firefox browser, CBE does not log you in and the rotation does not work.
- The download for the AWS root user is not available on the Chrome/Edge browser. When trying to log in as an AWS root user in the Chrome/Edge browser, CBE does not log you in and the password rotation does not work.
- The chromium extension instructions on the HSPAS portal is not working. The link to the detailed manual steps to install the extension does not work.

22.3 Release Notes

This update includes the following features, fixes, and other changes. Please also read the "22.3 Release Notes" on page 1202.

New Features

- Database Account operations are now successful on a SAP ASE Database with SSL enabled port when the correct trusted file is provided.

Documentation

Notice of Discontinuation

Resolved Issues and Changes in 22.3

- Fixed an issue where multiplexed accounts would not load properly for HSPAS users if there were a large number of them. (ref:425943)
- Fixed an issue where RDP sessions could cause connectors to overload the CPU. (ref:435461)
- Our previous version of Npgsql had a known issue of idle connections sometimes not getting cleaned up. We have updated the package to version 5.0.14 which fixes this issue. (ref:450990)
- Fixed an issue related to SSH login slowness that happened when using the native ssh client on AWS tenants and large number of systems are enrolled. (ref:453449)
- Added code to update clipboard permissions that were not working properly with the changes in the latest Chromium browser version. (ref:456764)
- Fixed an issue where a slow target system caused 100% CPU in the FreeRDP library. (ref:458050)
- Fixed an issue where discovery didn't find accounts on non-English language Windows systems. (ref:443308)
- Fixed an RDP copy and paste issue caused by updates to chromium-based browsers. (ref:463139)
- Fixed an issue where HSPAS would fail to install in a FIPS enabled environment. (ref:467224)
- Fixed an issue where accessing the workflow screen did not load any of the UI components. (ref:463070)
- Fixed an issue related to network latency when using WebRDP. (ref: 431794)

Supported Platforms

Cloud Connector

- Windows Server 2012r2, Server 2016, Server 2019, Windows 2022

Hyper-Scalable Privileged Access Service

- Windows Server 2016, Server 2019, Windows 2022

Windows PAS Remote Access Kit

Windows 10, Server 2012r2, Server 2016, Server 2019

Centrify App for Android

Android 5 (API level 21) and later

Centrify App for IOS

iOS 12 and above

Databases

- Microsoft SQL Server (versions 2008R2 and later)
- Oracle (versions 11.2.0.4, 12.1.0.1, 12.1.0.2)
- SAP ASE (version 16.0)

Network Devices and Appliances

- Check Point Gaia (versions R77.30, R80.10)
- Cisco AsyncOS (versions v10 and v11)
- Cisco IOS (versions IOS 12.1/IOS 15.0)
- Cisco NX-OS (version NX-OS 6.0)
- F5 Networks BIG-IP (versions v11, v12, v13)
- HP Nonstop OS (J06.19, H06.29)
- IBM i (versions IBM i 7.2, IBM i 7.3)
- Juniper Junos OS (version JunOS 12.3R6.6)
- Palo Alto Networks PAN-OS (versions 7.1, 8.0)
- VMware VMkernel (versions 5.5, 6.0, 6.5 and 6.7)
- Generic SSH

Desktop Apps

Privileged Access Service provides templates for the following Windows applications in the Desktop Apps feature. Privileged Access Service supports any versions of these applications that are compliant with the requirements for Windows Server 2012 R2 / 2016 Remote Desktop Services and RemoteApp. These applications must accept and process the command line strings pre-defined within the Desktop Apps templates. We have officially tested the following versions:

- SQL Server Management Studio (versions 13.0.15600.2, 2016 and 12.0.4522.0, 2012)
- TOAD for Oracle (version 13.0.0.80)
- VMware vSphere Client (version 6.0.0)

Note: VMware vSphere Client supports VMware VMkernel systems with a VMkernel system version below 6.5

Note: Custom user-defined templates are also available for additional desktop applications.

Known Issues

MFA Known Issues

- Ensure required data for each selected authentication factor is present When selecting the use of a secondary factor (SMS, phone, email, etc) you should ensure that the data is present in Active Directory for all users otherwise it is possible that users with missing data may be locked out. You can specify a preferred factor and if not present an alternative factor will be used. For example, if a user has no phone number in AD and SMS was the preferred factor, the Delinea PAS will fall back to another selected factor (for example, email). If there is no phone number or email in AD in this case, the user would effectively be locked out.
- Email as an MFA mechanism is subject to spam / junk filters Be aware that using email as an MFA mechanism may be affected by users' email providers' spam or junk filters.
- SMS / phone are only attempted once a password is validated This prevents spam and billing issues if an attacker attempts to brute force passwords to gain entry.
- For FIDO2 and On-Device Authentication options you will need to login from the tenant specific URL
- If you try to login to a system or check out a system's credentials using a workflow request, the request halts unexpectedly. However, you can still login or checkout if those rights are granted by policy.

Additional Information and Support

In addition to the documentation provided with this package, see the Delinea Knowledge Base for answers to common questions and other information (including any general or platform-specific known limitations), tips, or suggestions. You can also contact Delinea Support directly with your questions through the Delinea Web site, by email, or by telephone.

The Delinea Resources web site provides access to a wide range of information including analyst report, best practice brief, case study, datasheet, ebook, white papers, etc., that may help you optimize your use of Delinea products. For more information, see the Delinea Resources web site.

You can also contact Delinea Support directly with your questions through the Delinea Web site, by email, or by telephone. To contact Delinea Support or to get help with installing or using this software, send email to support@delinea.com or call 1-202-991-0540. For information about purchasing or evaluating Delinea products, send email to info@delinea.com.

22.2 Release Notes

This update includes the following features, fixes, and other changes. Please also read the "22.2 Release Notes" on page 1204.

New Features

Delinea and Centrify

We have updated the look and feel of the Cloud Client installer to reflect the new Delinea logo and colors. All files, folders, directories, settings, and registry keys and so forth remain as Centrify, as does the Admin Portal for PAS.

For more information about Delinea, see Delinea Announcement

Documentation

You can find the documentation at the Delinea Doc Portal, under the following sections:

- "Introduction to Cloud Suite and PAS" on page 1
- "Introduction to Cloud Suite and PAS" on page 1

We no longer provide a separate PDF for HS-PAS. Instead, the information is available in the "Deploying Customer-Managed (On-Premises) PAS" on page 219 section.

Notice of Discontinuation

None

Resolved Issues and Changes in 22.2

Here are the resolved issues and behavior changes in this release:

- Updated the bulkSystemDelete API to be more efficient.
- CVE-2018-1285 for log4net fixed with an upgrade to library version 2.0.14 in the Connector package.
- When checking for duplicate LDAP configurations, we now check both versions of LDAP so that we don't accidentally override LDAP1 configs with LDAP2.
- Fixed an issue with authenticating against a Radius server. Redirection will now use the correct user when attempting to authenticate.
- The optional "scope" field has been added in the partner management area. This field allows for integration with Azure Active Directory.
- Fixed an issue with the login screen in the iOS mobile app where it wasn't visible after updating the device to iOS 15.4.
- Fixed an issue that could cause ldap directory services to disappear from the list of directory services.
- When deleting systems, the email will now include information about failed deletions as well as successful ones.
- Updating LDAP and Google Directory Services configurations will now generate 'Modify' events that can be used to build reports and log changes.
- There is now a setup_certauth.ps1 script that you can use to add certificates (such as for smart cards) to your HS-PAS installation.

Resolved Issues and Changes in 22.2 HF1

Users can choose to delete previously pushed configuration files from PAS by navigating to Settings -> Resources -> Config files. Note that deleting config files from PAS does not revert the configuration files from the systems where those configuration files are.

For details about deploying configuration files, see "Viewing or Deleting Configuration Files" on page 767.

Resolved Issues and Changes in 22.2 HF6

Google released an update to Chrome that made users unable to handle copy and paste actions within RDP sessions. We have adjusted the permissions so that copy and paste are accessible to users again.

Resolved Issues and Changes in 22.2 HF7

- Added a new API to improve the performance of periodic password rotation.

Supported Platforms

Centrify Connector

- Windows Server 2012r2, Server 2016, Server 2019, Windows 2022

Hyper-scalable Centrify Privileged Access Service

- Windows Server 2016, Server 2019, Windows 2022

Windows PAS Remote Access Kit

Windows 10, Server 2012r2, Server 2016, Server 2019

Centrify App for Android

Android 5 (API level 21) and later

Centrify App for iOS

iOS 12 and above

Databases

- Microsoft SQL Server (versions 2008R2 and later)
- Oracle (versions 11.2.0.4, 12.1.0.1, 12.1.0.2)
- SAP ASE (version 16.0)

Network Devices and Appliances

- Check Point Gaia (versions R77.30, R80.10)
- Cisco AsyncOS (versions v10 and v11)
- Cisco IOS (versions IOS 12.1/IOS 15.0)
- Cisco NX-OS (version NX-OS 6.0)
- F5 Networks BIG-IP (versions v11, v12, v13)
- HP Nonstop OS (J06.19, H06.29)
- IBM i (versions IBM i 7.2, IBM i 7.3)
- Juniper Junos OS (version JunOS 12.3R6.6)
- Palo Alto Networks PAN-OS (versions 7.1, 8.0)
- VMware VMkernel (versions 5.5, 6.0, 6.5 and 6.7)
- Generic SSH

Desktop Apps

Privileged Access Service provides templates for the following Windows applications in the Desktop Apps feature. Privileged Access Service supports any versions of these applications that are compliant with the requirements for Windows Server 2012 R2 / 2016 Remote Desktop Services and RemoteApp. These applications must accept and process the command line strings pre-defined within the Desktop Apps templates. We have officially tested the following versions:

- SQL Server Management Studio (versions 13.0.15600.2, 2016 and 12.0.4522.0, 2012)
- TOAD for Oracle (version 13.0.0.80)
- VMware vSphere Client (version 6.0.0)

> VMware vSphere Client supports VMware VMkernel systems with a VMkernel system version below 6.5

> Custom user-defined templates are also available for additional desktop applications.

Known Issues

MFA Known Issues

- Ensure required data for each selected authentication factor is present When selecting the use of a secondary factor (SMS, phone, email, etc) you should ensure that the data is present in Active Directory for all users otherwise it is possible that users with missing data may be locked out. You can specify a preferred factor and if not present an alternative factor will be used. For example, if a user has no phone number in AD and SMS was the preferred factor, Cloud Suite will fall back to another selected factor (for example, email). If there is no phone number or email in AD in this case, the user would effectively be locked out.
- Email as an MFA mechanism is subject to spam / junk filters Be aware that using email as an MFA mechanism may be affected by users' email providers' spam or junk filters.
- SMS / phone are only attempted once a password is validated This prevents spam and billing issues if an attacker attempts to brute force passwords to gain entry.
- For FIDO2 and On-Device Authentication options you will need to login from the tenant specific URL .

Additional Information and Support

In addition to the documentation provided with this package, see the Delinea Knowledge Base for answers to common questions and other information (including any general or platform-specific known limitations), tips, or suggestions. You can also contact Delinea Support directly with your questions through the Delinea Web site, by email, or by telephone.

The Delinea Resources web site provides access to a wide range of information including analyst report, best practice brief, case study, datasheet, ebook, white papers, etc., that may help you optimize your use of Delinea products. For more information, see the Delinea Resources web site.

You can also contact Delinea Support directly with your questions through the Delinea Web site, by email, or by telephone. To contact Delinea Support or to get help with installing or using this software, send email to

support@delinea.com or call 1-202-991-0540. For information about purchasing or evaluating Delinea products, send email to info@delinea.com.

22.1 Release Notes

This update includes the following features, fixes, and other changes.

New Features

Ability to Deploy user.ignore and group.ignore Files to Multiple Systems

You can deploy the user.ignore and group.ignore configuration files to one or more enrolled Linux systems. You can deploy these files to individual systems or all systems in a set, and to no more than 500 systems at a time.

For details, see "Deploying the user.ignore and group.ignore Configuration Files" on page 688.

More Support for Local Linux Group Mapping

You can now map roles in Privileged Access Service to either new or existing Linux local groups. Previously you could map roles to just new local groups.

For details, see "Specifying UNIX Profile Information" on page 231.

Cloud Client Automatic Update Activity

When the Cloud Client attempts to do an automatic update, it will send the auto-update results to the target system's Activity tab. This will be available when the current version of the client (22.1) is automatically updated to a newer version.

Delinea Look and Feel

We have updated the look and feel to reflect the new Delinea logo and colors. All files, folders, directories, settings, and registry keys and so forth remain as Centrify.

Notice of Discontinuation

None

Resolved Issues and Changes

Here are the resolved issues and behavior changes in this release:

- Fixed an issue where in some cases the connector would not automatically restart after automatically upgrading to a new version.
- Fixed the issue where if you tried to elevate privileges for a user whose account name has 16 or more characters in it, privilege elevation failed with an error.
- Fixed an issue that might cause heavy database CPU usage intermittently.
- Fixed an issue where a user was prompted for user credentials twice when logging in to a system remotely using the "Enter Account" action.
- Fixed an issue that caused inconsistent Dark Mode behavior.

- Fixed an issue where running the report “User MFA Challenge Setup Status” might result in a query error.
- Fixed an issue where “Bulk Delete” might not delete some service accounts.
- Fixed an issue where the service didn't send Radius configuration information on connector startup.
- There are new reports related to privilege elevation activities; you can find these reports in the Resource Reports group.
- Fixed an issue where, under certain circumstances, if you tried to reset your password in the PAS Admin Portal by way of the Forgot Password option and there were multiple authentication challenges set up, the second required authentication challenge immediately skipped to the next step and failed.

Supported Platforms

Centrify Connector

- Windows Server 2012r2, Server 2016, Server 2019

Hyper-scalable Centrify Privileged Access Service

- Windows Server 2016, Server 2019

Clients for Linux

Client for Red Hat

- Red Hat Enterprise Linux 7.9, 8.3
- CentOS 7.9, 8.3
- Fedora 33, 34
- Oracle Linux 7.9, 8.3
- Amazon Linux 2 Latest Version

Client for Red Hat (ARM architecture):

- 7.9, 8.3

Client for SUSE

- SUSE15-SP3

Client for Debian

- Debian 9.13, 10.9, 11.2
- Ubuntu 18.04LTS, 20.04LTS, 21.04

Client for Alpine Linux

- Alpine Linux 3.14

> Before you uninstall the Centrify Client for Linux from an Alpine Linux system, you must unenroll the system first. The Alpine Linux package manager doesn't allow the service to verify that the client is unenrolled from Centrify PAS before uninstalling. If you uninstall the client without unenrolling first, you won't be able to log in to the system anymore.

Clients for Microsoft Windows

Windows 10 LTSB/LTSC, Windows Server 2012r2, 2016, 2019 LTSC, Windows 2022

Windows PAS Remote Access Kit

Windows 10, Server 2012r2, Server 2016, Server 2019

Centrify App for Android

Android 5 (API level 21) and later

Centrify App for iOS

iOS 12 and above

Databases

- Microsoft SQL Server (versions 2008R2 and later)
- Oracle (versions 11.2.0.4, 12.1.0.1, 12.1.0.2)
- SAP ASE (version 16.0)

Network Devices and Appliances

- Check Point Gaia (versions R77.30, R80.10)
- Cisco AsyncOS (versions v10 and v11)
- Cisco IOS (versions IOS 12.1/IOS 15.0)
- Cisco NX-OS (version NX-OS 6.0)
- F5 Networks BIG-IP (versions v11, v12, v13)
- HP Nonstop OS (J06.19, H06.29)
- IBM i (versions IBM i 7.2, IBM i 7.3)
- Juniper Junos OS (version JunOS 12.3R6.6)
- Palo Alto Networks PAN-OS (versions 7.1, 8.0)
- VMware VMkernel (versions 5.5, 6.0, 6.5 and 6.7)
- Generic SSH

Desktop Apps

Privileged Access Service provides templates for the following Windows applications in the Desktop Apps feature. Privileged Access Service supports any versions of these applications that are compliant with the requirements for Windows Server 2012 R2 / 2016 Remote Desktop Services and RemoteApp. These applications must accept and process the command line strings pre-defined within the Desktop Apps templates. We have officially tested the following versions:

- SQL Server Management Studio (versions 13.0.15600.2, 2016 and 12.0.4522.0, 2012)
- TOAD for Oracle (version 13.0.0.80)
- VMware vSphere Client (version 6.0.0)

> VMware vSphere Client supports VMware VMkernel systems with a VMkernel system version below 6.5

> Custom user-defined templates are also available for additional desktop applications.

Known Issues

Client Known Issues

- When you log in to an enrolled system and your account is set up to use MFA redirection, the service prompts you for your password, not the password for the MFA redirect user. This feature is available on systems that have the Centrify Client installed and enrolled.
- For privilege elevation workflow activity, the events in the Activity log show that commands were run without an authentication challenge when in fact the user was challenged with additional authentication requests when running the command after the workflow request is approved.

MFA Known Issues

- Ensure required data for each selected authentication factor is present When selecting the use of a secondary factor (SMS, phone, email, etc) you should ensure that the data is present in Active Directory for all users otherwise it is possible that users with missing data may be locked out. You can specify a preferred factor and if not present an alternative factor will be used. For example, if a user has no phone number in AD and SMS was the preferred factor, Cloud Suite will fall back to another selected factor (for example, email). If there is no phone number or email in AD in this case, the user would effectively be locked out.
- Email as an MFA mechanism is subject to spam / junk filters Be aware that using email as an MFA mechanism may be affected by users' email providers' spam or junk filters.
- SMS / phone are only attempted once a password is validated This prevents spam and billing issues if an attacker attempts to brute force passwords to gain entry.
- For FIDO2 and On-Device Authentication options you will need to login from the tenant specific URL .

Changes in HF1

Fixed a potential iOS mobile app notification issue.

Changes in HF2

Fixed an issue that alleviated system resources from exceeding optimal levels; the fix involved adding an index to a database table.

Changes in HF3

Fixed an SSH session heartbeat interval configuration issue.

An issue came about when a user who added the necessary permissions to a Secret Server vaulted account was not able to logon to any server resource due to a permission error. The reason this happened was because we did not elevate to search for the entity tied to the account (domain, database, etc.). The workaround was to add the view permissions to the entity tied to the account, but after the fix, it is no longer needed. We have fixed the way we view the Secret Server vaulted account, so that the workaround is not needed.

Improved performance related to checking user account permissions.

Changes in HF4

Fixed an issue with the login screen in the iOS mobile app where it wasn't visible after updating the device to iOS 15.4.

Fixed an issue that could cause ldap directory services to disappear from the list of directory services.