Delinea

Privilege Manager

Administrator Guide

Version: 11.4.x

Publication Date: 6/12/2024

Privilege Manager Administrator Guide

Version: 11.4.x, Publication Date: 6/12/2024

Table of Contents

Introduction to Privilege Manager

Privilege Manager is an endpoint least privilege and application control solution for Windows and macOS, capable of supporting enterprises and fast-growing organizations at scale. Mitigate malware and modern security threats from exploiting applications by removing local administrative rights from endpoints. The two major components are Local Security and Application Control.

Using Privilege Manager discovery, administrators can automatically discover local administrator privileges and enforce the principle of through policy-driven actions. Those policy-driven actions include:

- blocking, elevating, monitoring, allowing
- application quarantine, sandbox, and isolation,
- application privilege elevation, and
- endpoint monitoring

All this is seamless for users, reduce IT/desktop support workload, and support compliance obligations.

Privilege Manager does not require Secret Server or any other Delinea product to run. Secret Server's vaulting and workflow capabilities can be extended to privileged endpoint accounts when the two products are used together.

The typical user is part of an IT team that is tasked with implementing and overseeing a company's security business requirements and framework. In the product, this role is known as the Privilege Manager Administrator. Although there are a few other kinds of user roles that may use Privilege Manager now and then for minor tasks, the Privilege Manager Administrator is the main user of Privilege Manager.

It is useful (although not necessary) for Privilege Manager Administrators to be familiar with the basics of IT administration, such as the Group Policy feature from Microsoft.

Least Privilege Explained

Least Privilege is a security-driven management philosophy that models a system where all employees are given the minimum level of access rights necessary to carry out their job functions on endpoint machines. This is to protect each machine from malicious applications, rogue employees, or attackers. Privileged local admin or root accounts on endpoints give unfettered access to the entire endpoint and can potentially be used to access other computers, domain resources, and critical servers unless a least privilege security model is implemented. But implementing Least Privilege can be difficult for IT teams to enforce because there are plenty of daily, trusted activities that employees must perform that require access to privileged credentials.

Privilege Manager's toolset is two-fold. First, Local Security discovers all accounts that exist on endpoints and allows Privilege Manager Administrators to control the exact membership of every local group. This will ensure the correct admin and root accounts are permanently set. Additionally, credentials will be controlled by enforcing password rotation on those accounts.

Second, Application Control allows Privilege Manager administrators to manage application activity on endpoint machines. Applications that require admin rights or root access can be automatically elevated, allowed applications are allow listed, and malicious applications are blocked.

In other words, tailoring a robust, role-based Application Control system is key to keeping your organization's employees working both securely and effectively, without notable disruptions. But managing local administrator and

root accounts through Local Security is arguably the fastest way to lock down your network from malicious endpoint attacks that exploit administrator access.

Every implementation looks different when configuring Privilege Manager to work best for your organization. The key is to know your goal and be smart about getting there. The Getting Started section will walk you through beginning configurations for both Local Security and Application Control.

Feature Overview

Active Directory and Azure Active Directory

For those organizations leveraging Active Directory (AD) and/or Azure AD as their identity authentication and authorization service, deploying a least privilege program that works seamlessly with AD is absolutely critical. Privilege Manager integrates with AD so administrators can synchronize Domain Objects such as computers, OUs, and security groups from AD with their application control policies. Privilege Manager can leverage the user, group and privilege associations managed by Active Directory in its policy deployment and ensure unauthorized changes to AD made by workstation users, such as adding a user to a local administrator account, can be blocked automatically and in real time.

Agent & OS Reports

The Privilege Manager Agents are a critical component of Delinea's application control, giving you the ability to evaluate the health and status in real time. Privilege Manager provides pre-configured and fully customizable reporting on the status of agents and workstation operating systems. In the Privilege Manager reporting dashboard, you can drill into reports based on any dimension and easily export report data to other reporting applications or Excel.

Application Discovery for Administrative or Root Privileges

The most powerful applications installed on workstations are those that require administrator credentials or root privileges to run. Privilege Manager discovers all applications that run on workstations through its Learning Mode, giving you a precise snapshot of how these applications are used before you implement any changes. You can set up Discovery policies to target any new application action that requires administrator or root access, so no privileged action goes unnoticed.

Non-Domain Endpoint Support: Privilege Manager provides management and application control support for workstations even if they are not associated with your organizational network. Because it utilizes agents, it can manage workstations outside the network, such as those used by vendors, contractors, and partners, with the same dexterity and precision control as those within the network.

Automated Local Account Password Rotation

Rotate local account passwords on workstations based on a pre-defined, fully customizable schedule, ensuring that password best practices are followed.

Centralized Application & Execution Event Logging

Privilege Manager can record all executable events on managed workstations so you can review, search, and analyze these logs in a unified manner without leaving the console.

Child Process Control

Child processes are those that execute from within a file such as a PDF and are frequently how malware executes on a workstation. Privilege Manager allows you to prohibit execution of Child Processes to ensure unknown executables are restricted on your organization's network.

Custom & Scheduled Reports

Privilege Manager's ability to quickly generate fully customized reports and schedule the execution and delivery of these reports is essential to maintaining a real-time understanding of every aspect of your least privilege program.

Define Local Group Membership

Review and manage local groups, including Group membership. This powerful capability prevents Group membership changes from being made on a workstation, as all changes must be made via the Privilege Manager console.

End-user Justification & Admin Approval Workflow

This policy type requires that people provide a justification for why they need to run an application before elevating with administrator privileges. User Justification refers to the policy action. Since Conditions and Actions are independent, this action can be applied to any condition.

Flexible Policy Deployment Configuration

Enforce least privilege through policies for application control. You'll start with access to a broad library of out-of-the-box policies, all of which are completely customizable. Layered policies create the parameters that dictate precisely how privileges are accessed across your network. They define what actions people can run, and where. When policy conditions are met, Privilege Manager automatically applies an action (e.g. blocking, monitoring, application elevation, etc.) on one or multiple assets.

High Availability & Load Balancing

Web server clustering provides both high availability and load balancing by allowing multiple web servers to run Privilege Manager software. A clustered environment is key in disaster recovery scenarios as you can automatically failover to a separate web server with no downtime. Additionally, performance can be improved through load balancing by having multiple servers processing requests simultaneously.

Local Admin Rights Removal

Privilege Manager can automatically revoke all local administrative privileges on endpoints so you can adhere to a least privilege policy. With application-level privilege elevation, user-level privileges are not required and people can still access all the systems they need.

Local User Account Management

You can manage all local users on all endpoints across your organization, including the automatic rotation of local user password(s), all from a central console.

Local User & Group Activity Auditing

The ability to audit and review the activity of local users and groups is essential to retroactively identify problematic activity and reduce risk. Privilege Manager lets you swiftly review and search across all User and Group activity associated with privilege escalation on every managed endpoint.

Microsoft Entra ID Authentication

A new action, **Entra ID Authentication**, enables single or muli-factor authentication for Windows and macOS, using Microsoft Entra ID. This action is identified in the Application policy that requires Entra ID authentication. Refer to "Microsoft Entra ID Authentication" on page 506

Privilege Manager Mobile App

The Privilege Manager mobile app for iOS and Android lets you manage workstations, configure policies, process approvals, and receive event alerts via a mobile device so you can learn of requests and address issues quickly.

Real-time Application Analysis | Reputation Check

Privilege Manager integrates with reputation checking software like VirusTotal to provide application analysis in real time. This unique feature allows for reputation analysis of any unknown applications in order to mitigate risk of workstation attacks from ransomware, zero-day attacks, drive-by downloads, and other unknown malicious software. With Privilege Manager, all applications that meet a general condition (i.e. executed from a specific directory or directories, file names, types, or any applications that are disassociated with existing policies) can be sent to VirusTotal for a reputation check and analysis.

Responsive & Actionable Reporting Dashboard

Successful application control demands that you have a complete, real-time understanding of the status and activity of all workstations. Privilege Manager provides a unified reporting dashboard so you can quickly evaluate the status of workstations, review activity logs and event data, and access a broad library of reports. Responsive and fully configurable, Privilege Manager's dashboard reporting enables you to quickly drill down into reports across any dimension (time, geo-region, OS, status…) to evaluate activities and trends. From the dashboard you can also set up automated alerts to stay informed of potential problems.

Reverse Proxy

Many organizations choose to protect their Privilege Manager web server by restricting it from direct outbound internet access. To secure your environment according to best practices, it is not enough to simply set your server offline because Privilege Manager still will communicate directly to agents across your network that DO have direct internet access, therefore attackers can potentially use the connection between your endpoint agent and Privilege Manager to breach your web server. To prevent this direct connection between workstation agents and your Privilege Manager web server, Privilege Managers allows for the setup of a Reverse Proxy machine with limited permissions. A properly configured Reverse Proxy will act as a buffer between Privilege Manager agents and the Privilege Manager server to limit server exposure.

Sandboxing

Sandboxing quarantines applications so they are not allowed to execute, or only allowed to execute in a limited way so they don't touch any system folders or underlying OS configurations. Privilege Manager supports sandboxing for applications that are not known, to ensure they do not negatively impact productivity or introduce threats to the workstation or network.

ServiceNow

Many organizations leverage ticketing systems to streamline their support workflow and like to view and report on all support requests within a single system. Privilege Manager can be fully integrated into ServiceNow, so support requests and IT responses can be managed, tracked, and reported via the ticketing system itself.

Symantec Enterprise Platform (SEP)

For those organizations utilizing the Symantec Endpoint Protection or Symantec Endpoint Protection Cloud solution for allow listing and reputation, Privilege Manager can utilize the SEP allow list and reputation engine to inform and prescribe its provision of application control capabilities across workstations.

SysLog / SIEM

You can integrate your least privilege and application control program with a SIEM tool or other cyber security reporting and analytics services and tools. Privilege Manager can push out SysLog messages on a fully configurable schedule to any application or service that accepts the SysLog format.

System Center Configuration Manager (SCCM)

Privilege Manager can integrate with Microsoft System Center Configuration Manager and scan SCCM software delivery “packages” for applications that can be allow listed by Privilege Manager.

Tailored Block, Elevation, Justification, and Monitoring Policies

Privilege Manager supports allowing trusted applications, blocking to deny known malicious applications based on attributes, file hash, location, or certificates, and monitoring to prevent unknown applications from running. Monitoring provides a system for discovering the unknowns and adding an action that hinges on a reputation check. Distinct from allowing applications to run with default user level privileges, an elevation policy applies admin credentials to specified applications. This type of policy is often paired, so that employees can perform trusted tasks that require administrator credentials to complete, like installing a trusted application (Adobe) or device (printer), without involving IT support.

User Account Control (UAC) Override

By only elevating application privileges based upon specific policies and criteria, Privilege Manager ensures people don't use Microsoft's UAC capabilities to grant a dangerous or unknown application administrative rights under any circumstance.

Windows & Mac Account Discovery on Workstations

Privilege Manager identifies all local accounts on agent-installed workstations and flags those with local admin rights, including hidden or hard-coded admin privileges. A single, comprehensive view makes management easy.

Best Practices

The following links represent a compiled list of recommended best practices for Privilege Manager. You can reference these best practices as your system configuration is developed.

Administration

Security Algorithms

Introduces configurable "Security Algorithms" on page 479 through: Privilege Manager server settings, signature algorithms, and targeted agent settings.

Read and Write Access

Learn how to "Prevent Read and Write Access to File Types or Locations" on page 480 using this best practice.

Service Accounts and IIS App Pool

Delinea recommends "Using a Service Account to run the IIS App pool" on page 483.

Securing the IIS Server

This article presents a lit of items that can be implemented for "Securing the IIS Server" on page 492.

Active Directory

Active Directory Import - On-prem vs Cloud

"Status" on page 590 presents the nuances between on-prem and cloud import and provides instructions for each import.

Troubleshooting AD Sync

"Agent Registration" on page 585 includes troubleshooting for: authentication, duplicates, and resource type keys.

Application Policies

Policy Events

Refer to this article for best practices specific to policy events.

Policy Feedback

Using **Send Policy Feedback** helps administrators to gather data, analyze patterns, and then assign actions to application events retrospectively.

Optimizing Compile Times

This method of Optimizing Compile Times uses an Exclusion Path to the application control agent to safeguard against increased compilation times that affect system performance.

Secondary File Filters

As a best practice you create an elevate policy with a priority elevates or allows specific scripts or files to run. Refer to "Using File Inventory" on page 714.

Installation and Upgrades

Upgrades

Best practices for upgrades include: DB backup and TMS folder backup prior to an upgrade, as well as a repair solution for upgrade errors.

macOS

macOS System Preferences

Refer to this article for best practices specific to macOS System Preferences.

Notifications on macOS

The ability to manage notification settings on an endpoint allows the user to be able to see the notifications that privilege-manager sends out.

Navigating the UI

The Privilege Manager user interface, also referred to as the console, is launched in a browser. The URL to launch the user interface has the following form:

`https://[server-domain]/TMS/PrivilegeManager`

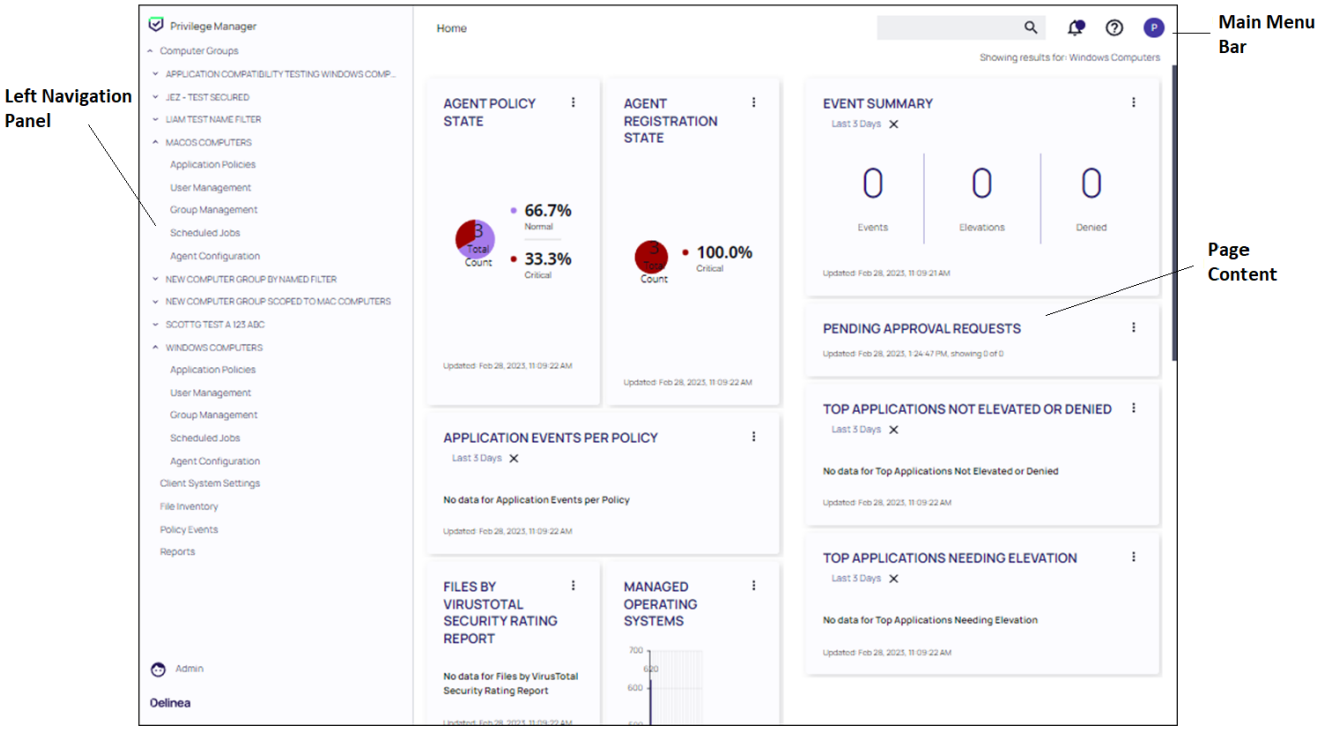
Where:

- server-domain, indicates the customer specific domain name, for example:
  - `https://mydomain.com/TMS/PrivilegeManager` for On-premises installations and
  - `https://myassignedname.privilegemanagercloud.com/Tms` for Cloud instances.

> **Note:** The User Interface (UI) seen by all <MadCap:variable name="global-vars.ProductName" /> roles is the same (whether Administrator or other). However, most of the interface is enabled only when you login in as a <MadCap:variable name="global-vars.ProductName" /> Administrator; the other roles are able to perform very few activities.

Upon login, the Home page is displayed in the page navigation area. At any point in navigating the application, click **Privilege Manager** in the left navigation panel to return to the Home page.

The functional areas of the UI are shown here. Refer to Navigation and Controls for detailed usage.



Left Navigation Panel

The left navigation panel provides access to all Privilege Manager functionality (e.g., computer groups, file inventory, administration).

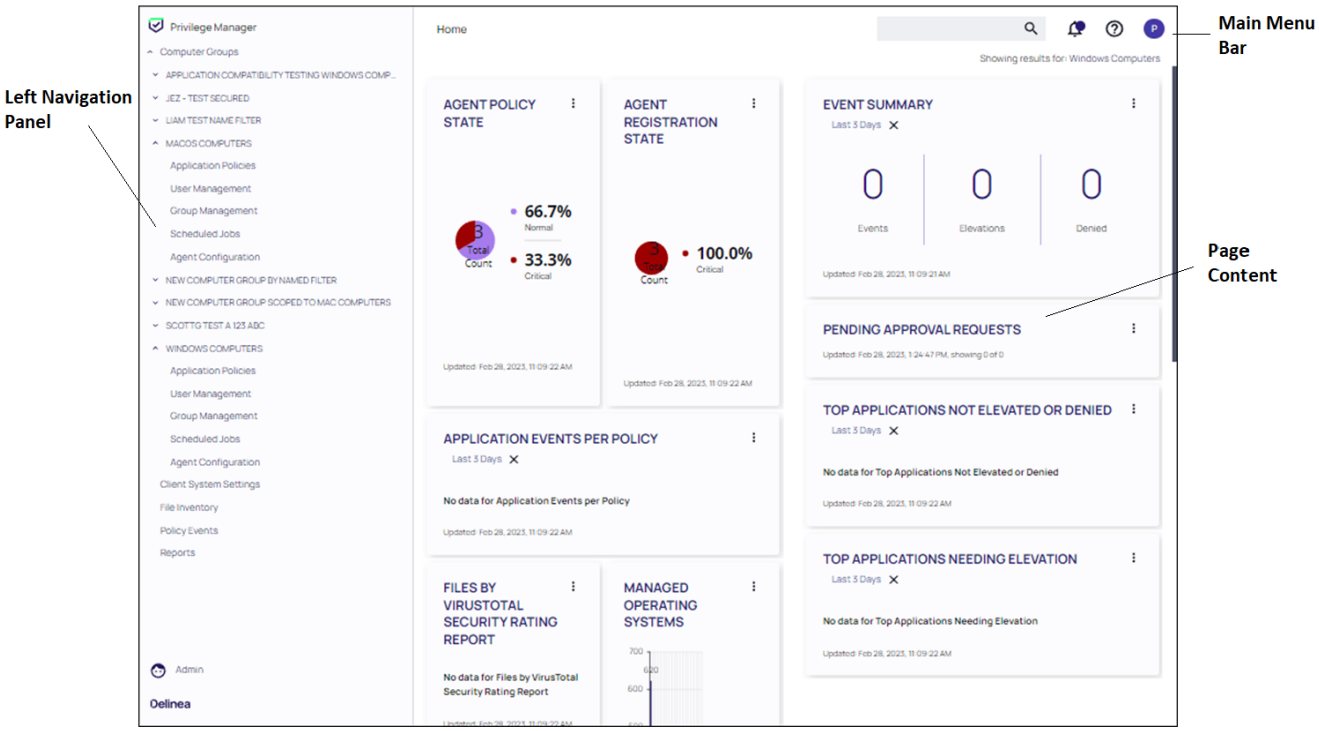
Main Menu Bar

The main menu bar, is present in the top right of all pages. It contains access to:

- Search
- Approvals and Notifications (see Managing Approvals and Managing Notifications)
- Help links to **About**, **Getting Started**, **Documentation** and **API Reference**.
- User Profile allows you to customize the UI and log out.

Page Content

Page Navigation and Controls present information for using controls on a page when performing tasks in the Privilege Managerapplication.



Accessibility

The Privilege Manager application has been enhanced to support accessibility features that include keyboard navigation in the left navigation panel and top menu bar, keyboard shortcuts, and screen readers that support tool tips and on-screen controls.

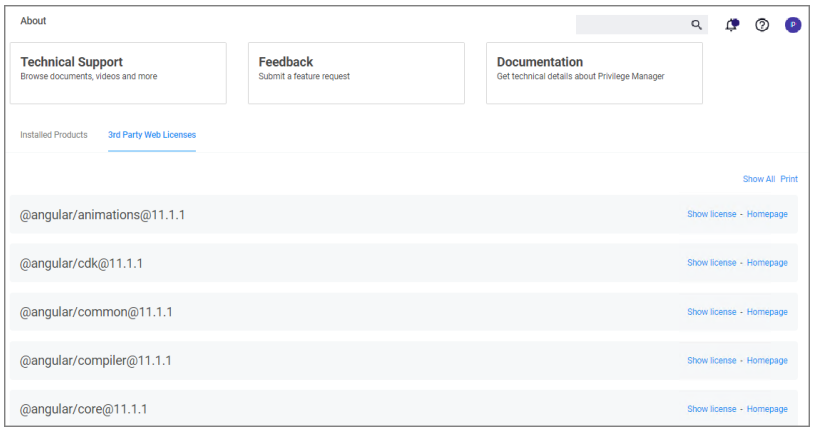
Use the Tab key to advance, or Shift + Tab key combination to move back when interacting with screen elements. This includes elements on the left navigation panel, top menu bar and tabs and fields on a page.

Viewing the About Page

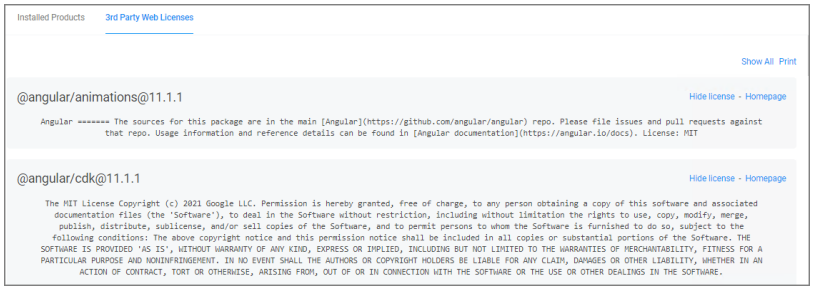
The About page provides navigation options to external sources such as the

- Support Portal
- Feedback
- Documentation

It further lists your currently installed Privilege Manager products.

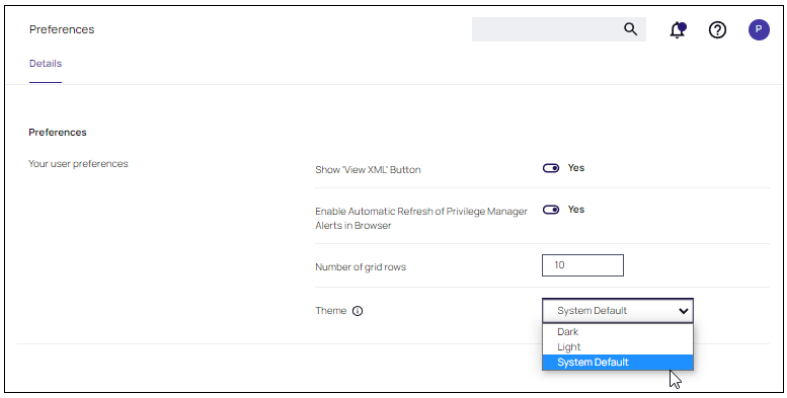


Under the **3rd Party Web Licenses** tab, you can review the 3rd party web licenses used by Privilege Manager. Use **Show All** to view details for all the licenses. Click **Print** to print a text file containing all 3rd party licenses and their details.



Customizing the UI

1. From the user profile icon (), click **Preferences**.

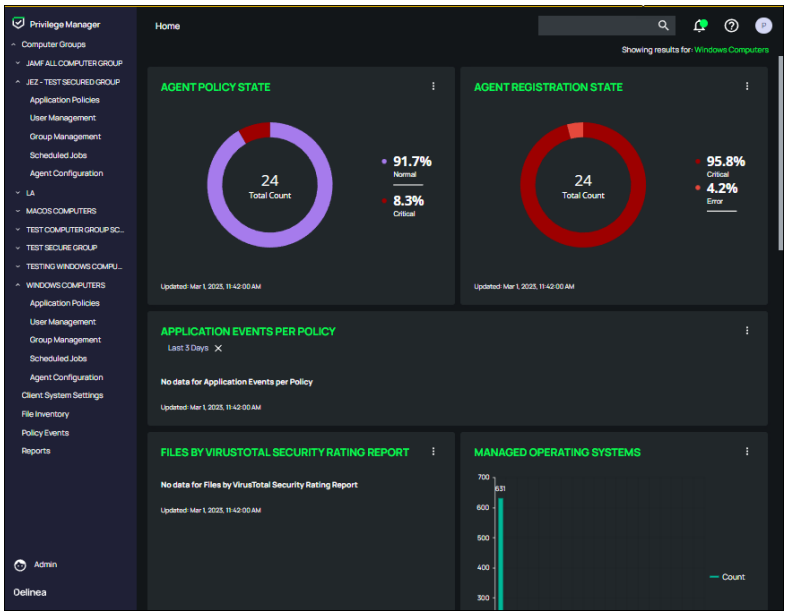


2. The Preferences page includes the following options:

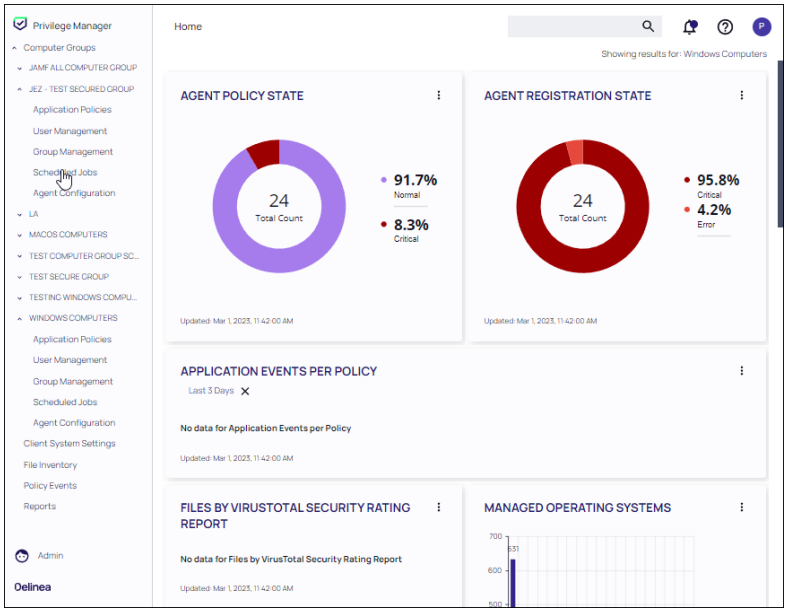
Option	Settings
Show 'View XML' button	When enabled (**Yes**), an additional menu option (**View XML**) is available when viewing a policy filter actions.
Enable Automatic Refresh of Privilege Manager Alerts in Browser	When enabled (**Yes**), entries displayed on the Alerts page are automatically refreshed when updates are made to Policy Alerts.
Number of gride rows	This value sets the maximum number of rows/page displayed for tables.
Theme	

3. At the **Theme** pull-down, select a theme. Refer to the examples shown.
   As its name implies, **System Default** ensures that the personalized colors you designate via the **Settings** page on your local machine dictate the Privilege Manager color theme. From a Windows machine, for example, navigate to **Settings**, select **Personalization**, click **Colors**, and **Choose your color** from the drop-down list box.

Dark Theme

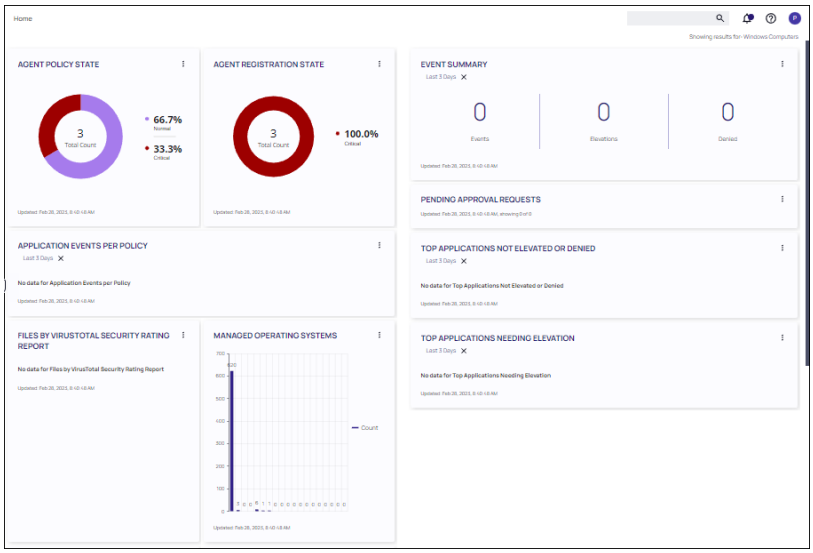


Light Theme



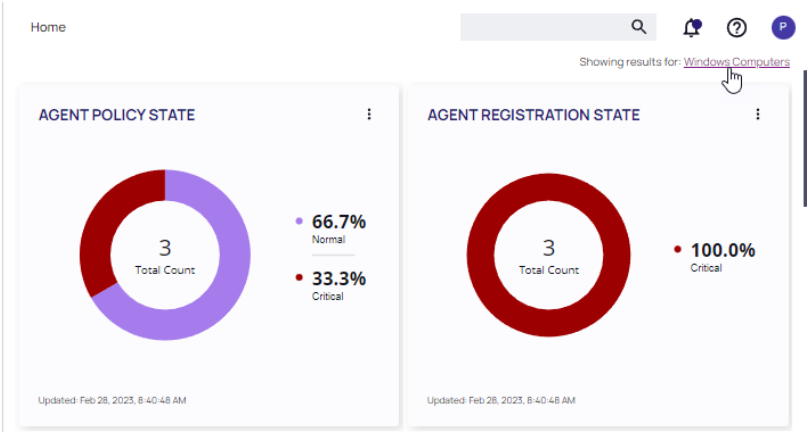
Home Page

The Home page consists of a dashboard with elements displayed for a selected computer group. The home page includes actionable dashboard elements as well as the gateway to the two major components of Privilege Manager, Local Security and Application Control. These are available from their respective tiles.



Adjusting Computer Group Display

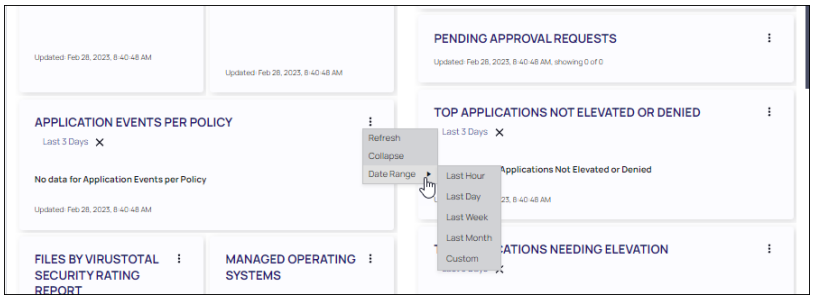
To update the display to a specific computer group, select that group in the **Showing results for** drop-down.



> **Note:** **AGENT POLICY STATE** displays counts for agents in the currently selected computer group, and does not directly relate to overall license usage. Therefore, this tile should not be used for a 1:1 comparison with the Utilization Summary in the Product Licenses report.

Viewing Component Details

Much of the text and other content on the page is clickable. The link under it will help you drill down to more detail. (Although some links, here and on other UI pages, are shown in blue, you should not assume that the absence of blue font implies there is no link. The best way to discover links is to hover over the content to find out if it is clickable.) The set of three little vertical dots, in the upper right corner of each tile, provide options to manipulate the tile.



Configuring Gauges

Many aspects Privilege Manager can be customized. The gauges displayed on the Home page of the Privilege Manager console and at many other pages can be removed and others can be added. The same with the Reports Options on the Reports page.

Gauges are used inPrivilege Manager to display the results of periodic configuration checks of the server and endpoints. Gauges allow reports and graphs to keep historical trend data, and speed up access in the console.

Reports and Gauges Available

Privilege Manager currently has gauges published to track when an agent last communicated with the server, agents that have received all of their policies, agents that have a random password set, etc.

You can click the following gauges to drill down for more information:

- Agent Policy State
- Agent Registration State
- Application Event Counts by Publisher
- Application Events Per Policy
- Event Summary
- Files by VirusTotal Security Rating Report
- Managed Operating Systems
- Pending Approval
- Top Applications
- Top Applications Needing Elevation
- Top Applications Not Elevated or Denied
- Top Denied Applications
- Top Users
- Top Users Attempting to Run Denied Applications

Navigation and Controls

In Privilege Manager, navigation and controls are aligned with Delinea's standard user experience. The main navigation menu is situated along the left side of your browser window and controls on each page are standardized.

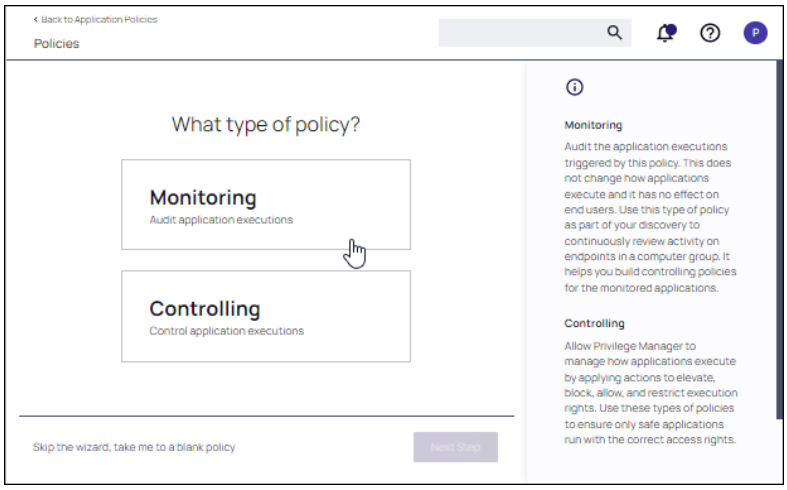
Purposefully arranged, each page contains functional and/or aesthetic modifications. The contemporary design and layout facilitate the ability to perform least privilege actions, leveraging a more straightforward approach, with intuitive actionable controls.

This all-inclusive application promotes a customer-first approach, simplifying the workflow process.

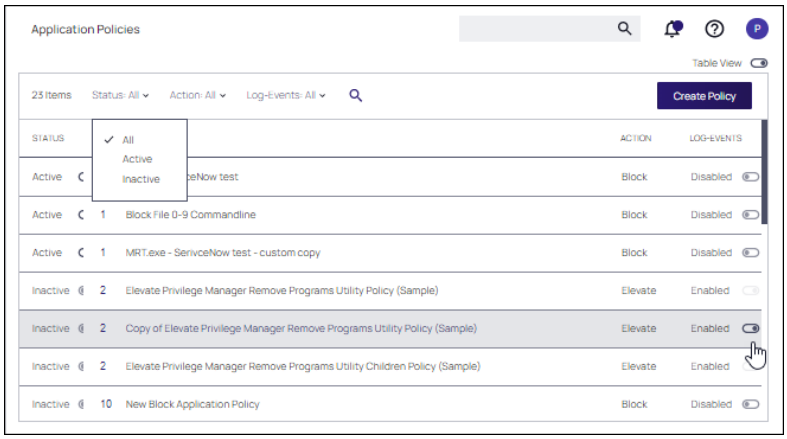
Features

- A neatly structured left navigation pane organized by computer group and commonly used features

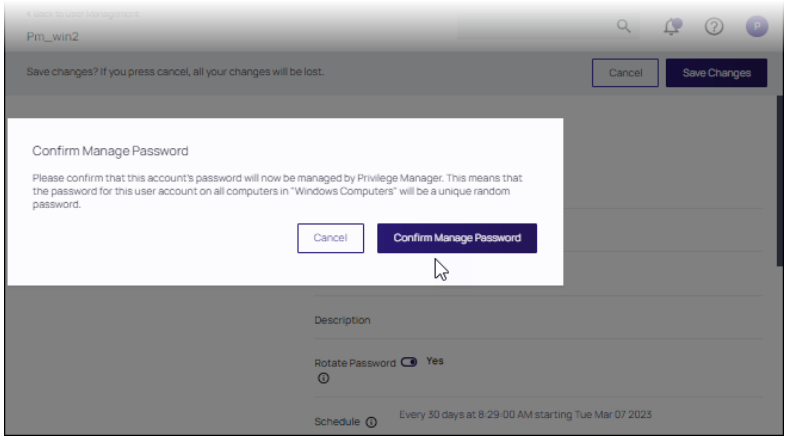
- Easily accessible application, group, and user policies, including a Create Policy wizard that provides complete guidance



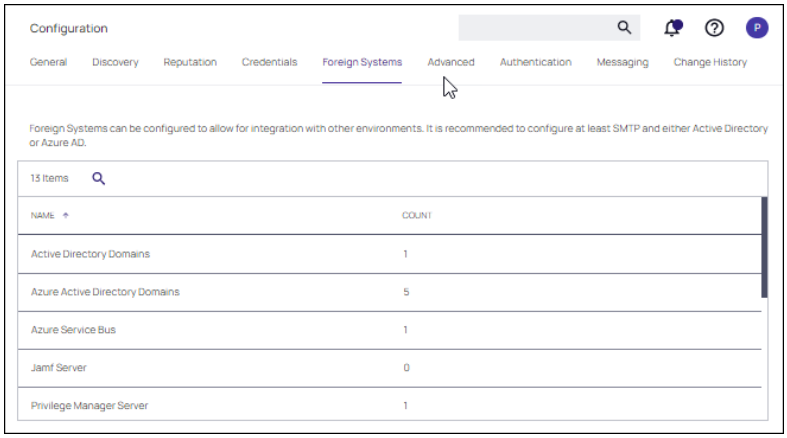
- Search and Filter options, and Context menus – each prevalent throughout the application



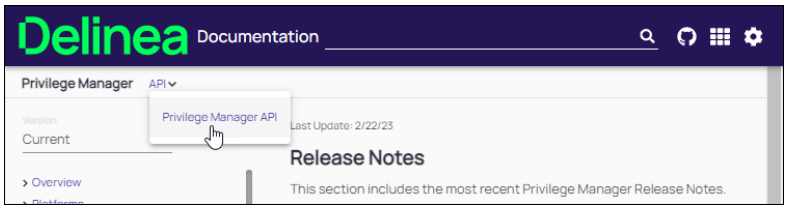
- Prominent actionable controls for Save, Create, Edit, Confirm.



- Tabular design for configuration details



- A publicly accessible API that allows you to invoke bulk operations specific to policies, filters, and actions

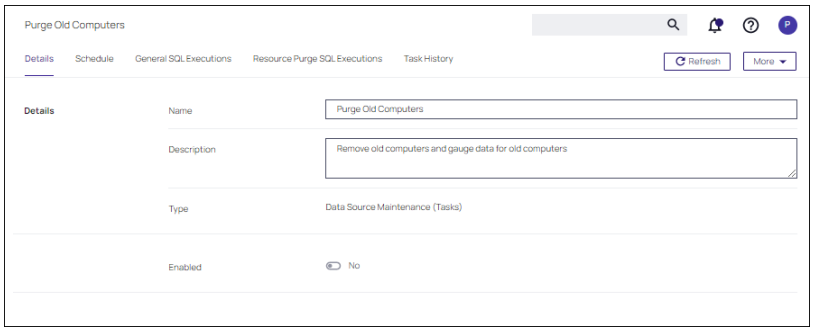


Managing Alerts

To access Alerts, click the icon and select **Notifications** from the menu options.

Alerts are listed by priority and category such as Unacknowledged Events, Pending Approvals Count, Number of Application Events, Install Agents, etc. Item in the list indicate the status of the notification as good (green), needs attention (yellow) and failed (red).

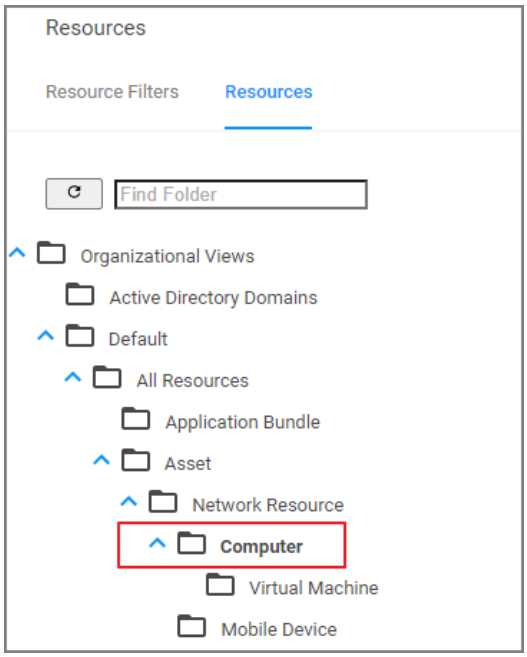
Click any notification to view its details, schedule, execution, and task history.



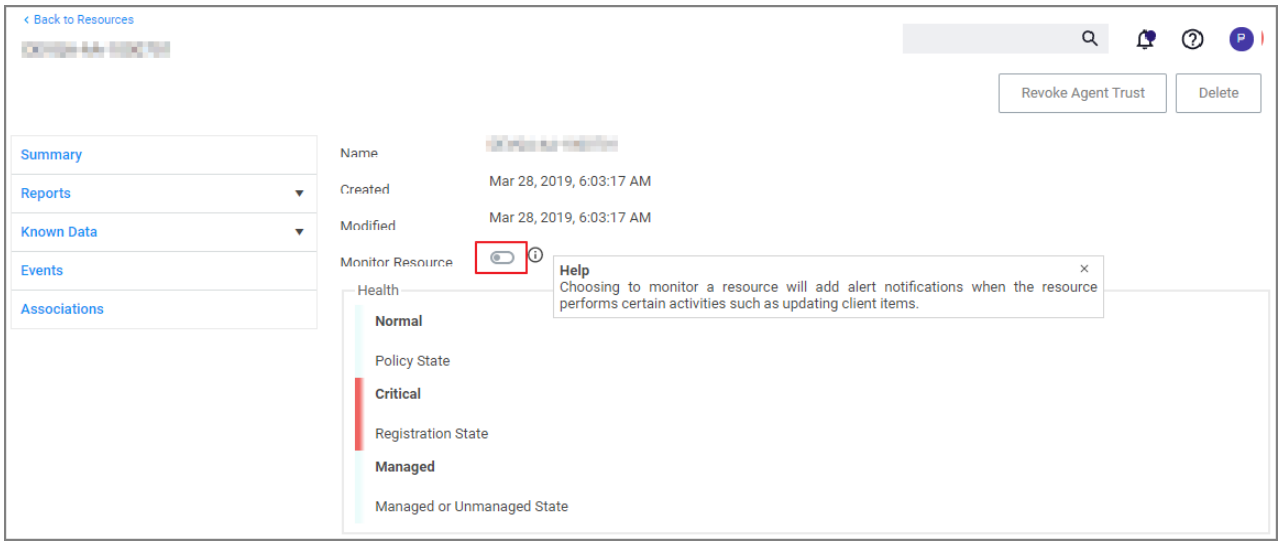
Workstation-Specific Alerts

Alert Notifications can also be triggered for a specific agent workstation, if the computer resource was configured for monitoring.

1. Navigate to **Admin | Resources**.
2. On the **Resources** tab, open the **Computers** folder.



3. From the list select the workstation you with to monitor and open the Resource Explorer for that endpoint.
4. Set the **Monitor Resource** switch to active. images/alert-monitor.png



Once monitoring is enabled, alert notifications for the agent workstation are available. These type of alerts inform about the agent registration, resource discovery, and update retrieval times.

macOS Alerts

For macOS workstations on Catalina or later, Administrators might want to follow Best Practices: Manage Privilege Manager Notifications on macOS

Clearing Alerts

Alerts cannot be deleted. However, if a filter is not being used, it can be deleted from a policy, which will clear the filter and the associated alerts.

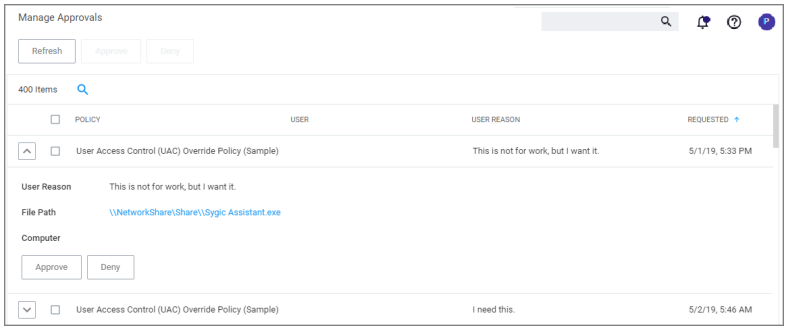
Managing Approvals

Approvals are created in **Admin | Approvals**. For example:

- Endpoint Group Member Approval Action
- Group Member Approval

Approvals are managed on the Manage Approvals page, that you can accessed in either of two ways.

- Click the Alerts icon and select **Manage Approvals** or
- Select **Admin | Manage Approvals** in the left navigation panel.

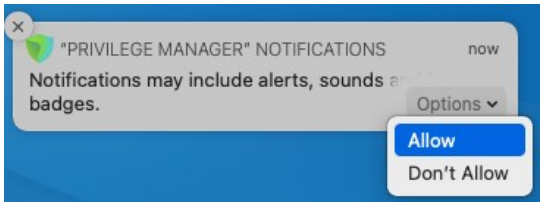


Selecting a Disposition

Use the expand/collapse icon (up/down chevron) to view approvals. Click **Approve** or **Deny** as required.

Best Practices: Manage Privilege Manager Notifications on macOS

As of macOS Catalina, Apple provided the ability to manage notification settings in macOS by using Configuration Profiles. The benefit of managing this setting is that you as the administrator have complete control over the desired state of that configuration on the endpoint. You want the user to be able to see the notifications that Privilege Manager sends out. If the setting is not managed the user may miss something important, if they previously clicked **Don't Allow**.



The example Manage Notifications XML snippet provided can be used and is based on the following property values. Depending on your chosen MDM provider, the example snippet might need editing.

- **AlertType** : 1 (Temporary Banner)
- **BadgesEnabled :** true (Enables the badge to be displayed for Privilege Manager)
- **BundleIdentifier** : com.thycotic.privilegemanagergui
- **CriticalAlertEnabled** : true (Enables critical alerts that can ignore the Do Not Disturb feature)
- **ShowInLockScreen :** false (For privacy concerns it is recommended to not show in lock screen)
- **ShowInNotificationCenter** : true (Enables notifications in the notification center for this app)
- **SoundsEnabled** : true (enables sounds for this app)

Manage Notifications XML


```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.
com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
        <key>PayloadContent</key>
        <array>
            <dict>
                <key>NotificationSettings</key>
                <array>
                    <dict>
                        <key>AlertType</key>
                        <integer>1</integer>
                        <key>BadgesEnabled</key>
                        <true/>
                        <key>BundleIdentifier</key>
                        <string>com.thycotic.privilegemanagergui</string>
                        <key>CriticalAlertEnabled</key>
                        <true/>
                        <key>NotificationsEnabled</key>
                        <true/>
                        <key>ShowInLockScreen</key>
                        <false/>
                        <key>ShowInNotificationCenter</key>
                        <true/>
                        <key>SoundsEnabled</key>
                        <true/>
                    </dict>
                </array>
                <key>PayloadDisplayName</key>
                <string>Notifications</string>
                <key>PayloadIdentifier</key>
                <string>8BC5EB47-8E9B-4CCB-BFB8-
7ED346060748.com.apple.notificationsettings.510D70CC-A4DE-42FB-B327-CAA358740DF7</string>
                <key>PayloadOrganization</key>
                <string></string>
                <key>PayloadType</key>
                <string>com.apple.notificationsettings</string>
                <key>PayloadUUID</key>
```

```
                <string>510D70CC-A4DE-42FB-B327-CAA358740DF7</string>
                <key>PayloadVersion</key>
                <integer>1</integer>
            </dict>
        </array>
        <key>PayloadDisplayName</key>
        <string>Approve Privman Notifications</string>
        <key>PayloadIdentifier</key>
        <string>com.thycotic.com.8BC5EB47-8E9B-4CCB-BFB8-7ED346060748</string>
        <key>PayloadOrganization</key>
        <string>Thycotic</string>
        <key>PayloadScope</key>
        <string>System</string>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>8BC5EB47-8E9B-4CCB-BFB8-7ED346060748</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
    </dict>
</plist>
```


Left Navigation Panel

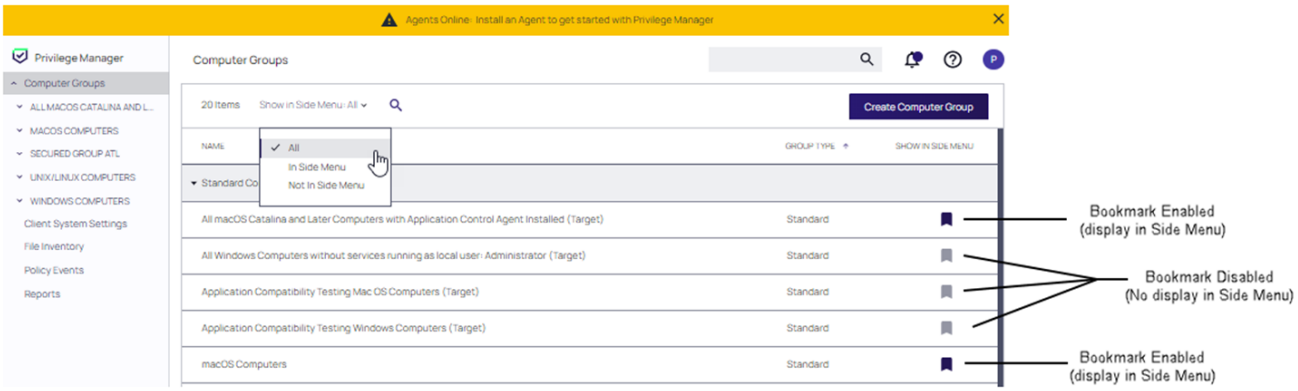
The left navigation panel is used to move between functional areas in the Privilege Manager application. These areas include:

- Computer Groups
- System Settings and Inventory
- Administration

Computer Groups

Computer Groups provide endpoint management and application control for your workstations. Click **Computer Groups** at the top of the left navigation pane. The Computer Groups table in the Page Content area updates to display all currently defined computer groups.

> **Note:** Each computer group in the table has a bookmark setting that can be enabled or disabled. If a bookmark is enabled, it is displayed in the left navigation pane. Disabling a bookmark removes the computer group from the left navigation pane.



Expand the tree under each computer group in the left navigation panel to display subitems organized by:

- Application Policies
- User Management
- Group Management
- Scheduled Jobs
- Agent Configuration

Client System Settings, Inventory, and Reports

Features for viewing system settings, inventories and reports relating to system states are provided as selections in the left navigation panel. Specifically:

- Client System Settings - These are common settings for standard Windows user computers ranging from allowing installation of drivers to printers. These settings are deployed to Agents the same as any Policy.
- File Inventory - This page lists all external files used with the application and their metadata.
- Policy Events -
- Reports - Select **Repprts** from the left navigation panel to display an array of reports that include: actions, agents, diagnostics, and security.

Admin Menu

Select **Admin** at the bottom of the left navigation panel. The Admin menu provides access to **Tools**, like:

- Disclose Password
- Manage Approvals
- "Offline Approvals" on page 282

The other available **Admin** subitems are:

- Actions
- Agents
- Config Feeds
- Configuration
- Diagnostics
- File Upload
- Filters
- Folders
- Import Items
- Licenses
- Personas
- Resources
- Security
- Secret Server - only available if integrated via Foreign Systems
- Server Logs
- Setup - only available for On-premises instances
- Tasks
- Users

Installation and Upgrades

This sections contains all you need to know about installation and upgrading Privilege Manager and all its components.

Note: Privilege Managerexclusively supports operating systems (OS) that have not reached their official End of Support. For optimal performance and compatibility, it is recommended to utilize Privilege Manager on a supported and actively maintained OS.

The following topics are available:

- System Requirements
- "Reboot Requirements - Windows Agents" on page 29

Licensing

Cloud Licenses

Licensing for Privilege Manager Cloud customers is managed via Delinea.

Installing New Licenses - On-premises Only

To install new Privilege Manager licenses, it will depend on whether you chose to;

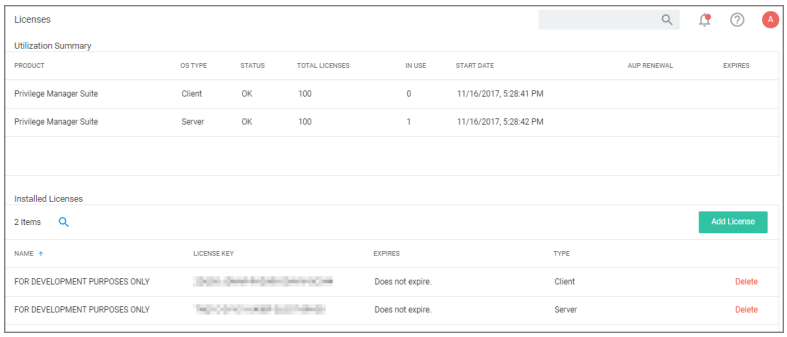
- perform a standalone install, or
- install Secret Server in tandem with Privilege Manager.

Note: Online activation is not required for Privilege Manager licenses.

Steps for Standalone Privilege Manager Installation

To install licenses without Secret Server:

1. Navigate to **Admin | Licenses** or **click** the Product Licenses Installed link in the top banner.



2. On the Privilege Manager Licenses page, click **Add License**, then either:
   - enter your License Name(s) and Key(s) one at a time:

   or

   - use the **Add license certificate instead** option.

3. Click **Add**.

Steps for Combined Secret Server + Privilege Manager Installation

To install licenses with Secret Server on the same server as Privilege Manager, you will need to install licenses through the Secret Server UI and then import the new licenses into Privilege Manager.

1. To access Secret Server's licensing page, either click the Secret Server link listed in the banner at the top of the Secret Server Licenses page or in Secret Server navigate to **Admin | Setup - Licenses**.
2. On Secret Server's License page, select **Install New License**.
3. Enter your **License Names** and **Keys** individually or through the Bulk Entry Mode.
4. Click **Save** or **Add Multiple Licenses** to save the License Keys. Installing these licenses in Secret Server will automatically import the licenses into Privilege Manager.
5. Navigate back to the Privilege Manager License page to verify under:

   Tools | Privilege Manager| Admin | Privilege Manager-Licenses.

   Note: If your license keys do not appear or you have too many keys listed, click the import task link and then run task to reset.

Converting from Trial Licenses

If you previously had evaluation licenses and recently purchased, you will need to install your new license keys for production via the same steps as above. Normal trial licenses offer 50 endpoint agents and expire 30 days after issue.

Expired Licenses

When your Privilege Manager licenses expire or have exceeded the licensed count, Privilege Manager will stop processing new inventory and application control events. Endpoints will continue to enforce policies.

In your Installed Licenses list use the **Delete** option to remove expired or old licenses that are not in use anymore.

Client vs. Server Licenses

- **Client License**: This license provides coverage for endpoints that are workstations, such as Windows 10, windows 7, macOS or Unix/Linux endpoints, etc.
- **Server License**: This license provides coverage for endpoints that are server machines, Windows Server 2019, Windows 2016, etc.
- **Support License**: Without having a support license you will not be able to complete upgrades and will not be able to receive support or maintenance.

License Expired or Exceeded License Count

The Server will stop accepting data sent from agents that are in violation of the licensing based on operating system license counts. New endpoints will register, but will not be recorded, which means the endpoint:

- Will not get added to the resource targets and will not collect application or user inventories
- No password changes will occur, etc.
- Policies will run on the endpoint, but the server will completely discard the data, and it won't be stored.
- Tasks will not run – all automation will stop and event Discovery will not inventory users or applications, new endpoints won't be discoverable.

An exceeded license count is indicated with a warning banner.

10.7 and up Reset Licensing

If you need to reset licenses for your Privilege Manager instance refer to the Reset Licensing topic.

Software Downloads

This page provides links to DelineaPrivilege Manager product and agents software downloads.

Note: Delinea supports the use of software versions up to a year prior to the current version. You can find the documentation for previous versions here.

Server Software

Version	Product
12.0.0	Combined Secret Server and Installer - Authentication required!
	Privilege Manager Application Files - Authentication required!

Agent Software

Windows Workstations

Agent Version	Product
12.0.1016	Bundled Privilege Manager Agent Installer - Windows
12.0.1016	Core Thycotic Agent (x64)
12.0.1016	Core Thycotic Agent (x86)

Agent Version	Product
12.0.1016	Application Control Agent (x64) [*1]
12.0.1016	Application Control Agent (x86) [*1]
12.0.1016	Local Security Solution Agent (x64)
12.0.1016	Local Security Solution Agent (x86)
12.0.1016	Bundled Privilege Manager Core and Directory Services Agent - Windows
12.0.1002	Directory Services Agent (x64)

- [1]: Do not update to version 12, if workstation runs Windows 10 version 1507.

macOS Workstations

Note: Privilege Manager version 12.0.0 is the last version of the Mac agent to support macOS 10.15 Catalina, for which Apple has not released a security update since July 2022. Going forward,Privilege Manager will follow the common practice of supporting those OS versions that Apple itself supports with security updates, namely, the current and two previous versions of macOS. (We anticipate discontinuing support for macOS 11 Big Sur when we implement support for the next release of macOS in late 2024.) We encourage our users to upgrade to a supported version of macOS to continue receiving the latest features and security updates.

	Product	OS Version Support
12.0.0.056	Privilege Manager macOS Agent	Catalina and later using System Extensions (Apple silicon & Intel)

Note: Privilege Manager no longer supports Unix/Linux. While you can download the agent, there will be no additional agent updates.

Privilege Manager System Requirements

These are requirement for an on-premises integration.

Note: Verify that the .NET version between the Privilege Manager and Database Server in use are matching, especially if installed on different Windows Server versions.

Important: The user Privilege Manager uses to connect to the database must be a sysadmin during installation or upgrade.

Minimum Requirements

Web Server	Database Server
4 CPU Cores	4 CPU Cores
8 GB RAM	16 GB RAM
40 GB Disk Space	150 GB Disk Space
Windows Server 2012 R2 or newer	Windows Server 2012 R2 or newer
IIS 7 or newer	SQL Server 2012 or newer
.NET 4.6.1 or newer	
Powershell 3.0 or newer	

Recommended Requirements

Note: Environments with over 25,000 Endpoints require a scoping call with a Delinea engineer.

Web Server	Database Server
8 CPU Cores	8 CPU Cores
32 GB RAM	64 GB RAM
40 GB Disk Space	500 GB Disk Space
Windows Server 2016 or newer	Windows Server 2016 or newer
IIS 7 or newer	SQL Server 2012 or newer
.NET 4.6.1 or newer	
Powershell 5.0 or newer	

Client Requirements

For details refer to the Agent specific system requirements as provided under these topics:

- macOS Endpoint System Requirements
- Windows Endpoint System Requirements
- RAM, CPU, and Disk Space - negligible

Details

- System Requirements apply to both physical and virtual machines.
- For best performance, we recommend using dedicated (clean) servers for Delinea products.
- PowerShell must be allowed to execute and cannot be blocked on the server or the endpoint by other products.
- If .NET and/or IIS features are not already installed on the web server, the Delinea Installer will add and configure them automatically.
- If SQL is not already installed on a database server, the Delinea Installer can setup SQL Express on the web server, however SQL Express is intended for Trials and Sandbox environments ONLY. Though Delinea will support SQL Express, users will likely experience performance issues due to the memory and product limitations. If experiencing performance issues while using SQL Express, it is highly recommended to upgrade to SQL Server prior to contacting Delinea Support.
- A link to Microsoft documentation on the use and limitations of SQL Express can be found at: https://docs.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-2017
- Web Servers that are NOT supported: Small Business Server (SBS), The Essentials Edition, Domain Controllers, Sharepoint Servers.

Ports/Agent Access Information

- **Outbound (port 443 - HTTPS)**: This is the default access port through which the agent connects to the server. You may specify a different port based on your environment.
- **Inbound (port 5593)**: The is the default and only port that the agent listens on. This port is not required and you can block port 5593. If you block the port, the agents pull updates from the server based on a set schedule.
- **SQL (port 1433)**: This is the default SQL DB port. The SQL port can be customized.

Reboot Requirements - Windows Agents

Important: When installing the agent for the first time or upgrading from a previous version, read this entire topic to understand what conditions in the runtime environment will result in a required reboot of the computer in order for the install/upgrade to be completed properly and the agent to function properly. Failing to understand the reboot requirements in relation to your environment may result in the application control service or other components of the agent failing to function properly.

The Privilege Manager agent for Window is composed of a mix of .NET managed code and native C++ code built into various binary format EXE and DLL files. Some of the binaries run as native NT services, such as **Thycotic Agent** (Core Agent) and **Thycotic Application Control** (ACS), while others run on the user's interactive desktop, such as the **Agent Utility**, **JIT Mode Manager**, and the various "helper apps" which display the justify/approval UI or the application denied/blocked messages. Additionally, some of the DLLs are loaded into PowerShell as modules when various scheduled tasks are executing, while others are loaded into processes running applications which have had various actions applied to them such as **Restrict File Dialogs** or **Block Local User/Group Management**, or were launched with Admin rights under JIT, were subjected to justify/approval requirements, etc. Finally, there is a DLL that gets loaded into Microsoft's AppInfo (Application Information) service, where the majority of UAC functionality is implemented, so that the agent can intercept the UAC consent prompt when performing elevation operations.

When the agent is installed for the first time, there are no concerns about existing agent-related files being held open such that a reboot is required to replace them with newer versions. However, the **AppInfo** service will not have our DLL loaded into it to intercept the UAC consent prompt until a reboot has been performed. It is not sufficient to simply stop the **AppInfo** service and then restart it. This effectively means that a reboot is always required. It should be noted that by default, the **AppInfo** service, which is implemented in a DLL and loaded by an instance of **SVCHOST.EXE**, is configured to run in a shared process which also hosts other native NT services. Attempting to avoid the reboot by simply killing the service host process to force the service to be restarted will cause undesirable collateral damage that only further necessitates a reboot.

When the agent is upgraded, the native NT services for **Thycotic Agent** and **Thycotic Application Control** are both stopped by the installer. However, the **AppInfo** service does not get stopped and cannot be stopped by the installer. Also, the number of application processes running on the computer that may have other agent-related DLLs held open because of application control logic having been inserted into them is completely non-deterministic. To further complicate things, it is possible for a scheduled task to execute in a non-deterministic manner while the agent installer is running. The result is that any upgrade of the agent is guaranteed to have one or more files held open which cannot be replaced until the computer is rebooted. Attempting to restart the Thycotic Agent and Thycotic Application Control services will result in either or both failing to function properly because of loading a mixture of outdated and updated DLLs. One frequent problem that has been observed is that the **Thycotic Application Control** service starts but does not function properly and consumes excessive amounts of CPU time. Additionally, if the **AppInfo** service is still running with the old agent-related DLL loaded into it, the handling of elevation operations involving interception of the UAC consent prompt may fail to function properly.

It should be noted that the interactive combined installer will prompt for a reboot if it detects that certain files are locked, but due to some quirky behavior in how **MSIEXEC.EXE** works, there are times when the installer will not report a reboot as required when one is required. For the separate or combined MSI packages, there are command line parameters that can be provided to suppress an automatic reboot when one has been determined to be required, but the same caveats apply regarding the agent's various components failing to function properly until a reboot has been performed.

This behavior is 100% normal and has been common to the Windows platform going all the way back to 16-bit Windows 3.1. As such, it is not a defect with the agent nor its installer. Bug reports should never be filed due to a reboot being required to complete an install/upgrade. When planning to deploy the agent in an enterprise environment, the need to reboot the computer should be accounted for up front to minimize downtime and interruptions for end users.

Basic Installation

Prerequisites

ASP.NET Website

Privilege Manager is installed as an ASP.NET website. The setup.exe file will set up the website with the correct permissions and create the settings in IIS.

SQL Server Database

Delinea products require an instance of SQL Server for the database backend and an instance of SQL Server Express will be installed by the setup.exe file, if missing. However, it is strongly recommended to not use SQL

Server Express for production environments. SQL Server Express edition is intended for Sandbox and trial environments, Delinea recommends purchasing SQL licensing for use in production environments.

A SQL account is required. If that account has the db_creator role, the installer can create the database during the installation. Alternatively, if the blank database was manually created before running the installer, the SQL account will require db_owner of the database. If using Windows authentication with the database, the SQL account will be the app pool service account.

Administrative Access

Throughout the installation process, you will be required to be an administrator to perform most actions. Please ensure that you are logged onto your system with a Windows account that has administrative rights before beginning your install.

Additional Recommendations

1. Use an SSL certificate for Privilege Manager.
2. Run Microsoft Update on your server to make sure all components are up to date.

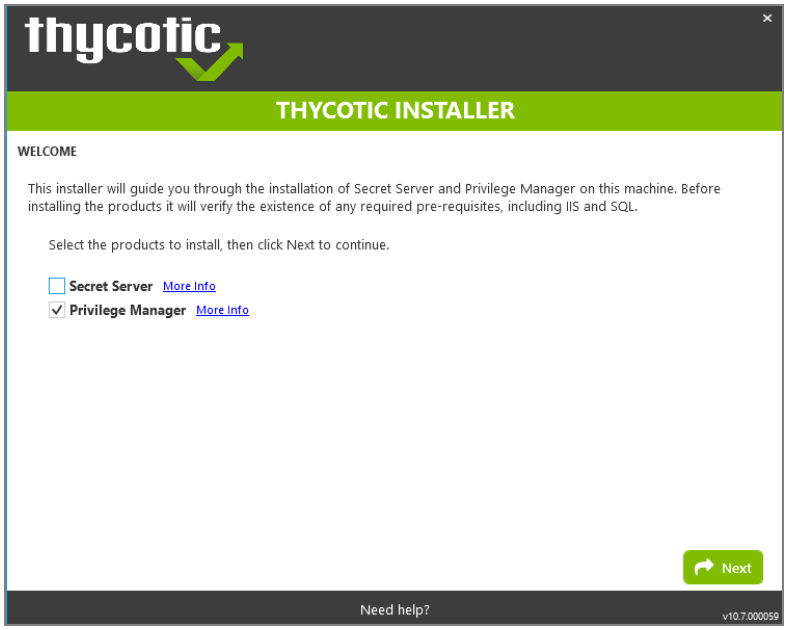
Download the Latest Version of PM Installer

The latest version of Privilege Manager is available for download under the Software Downloads topic. It is recommended to run the downloaded setup.exe file as an administrator.

> **Note:** When installing Privilege Manager against SQL 2022, ensure the SQL Server and SQL Server CEIP services have been set to a startup type of Automatic and not Automatic (Delayed Start). The startup type can be checked under services.msc on the SQL Server.

Running the Installer

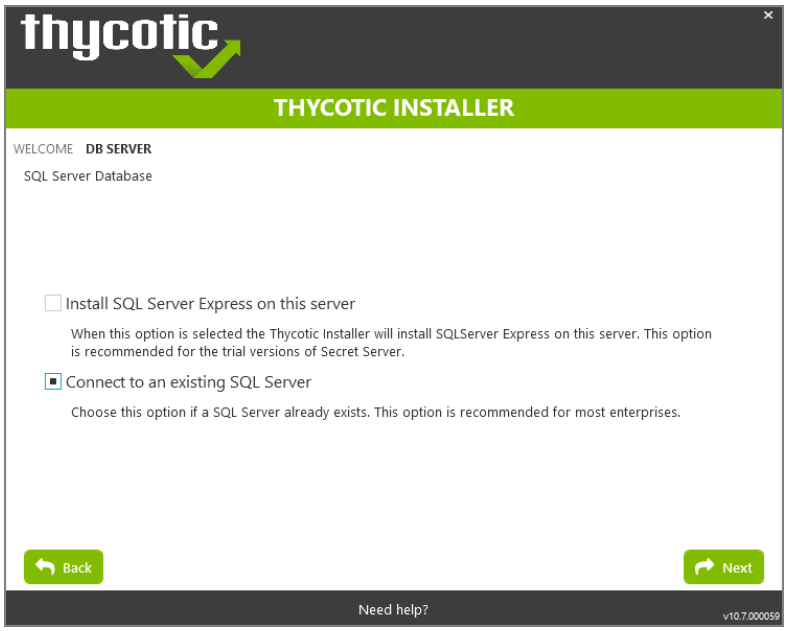
1. Double-click the downloaded setup.exe to run the installer. The installer opens on the **Welcome** tab:



2. Verify that the Privilege Manager box is checked.

   Note: Privilege Manageras a standalone product comes with three roles Administrator, Basic User, and Help Desk User roles. Please refer to Application Roles.

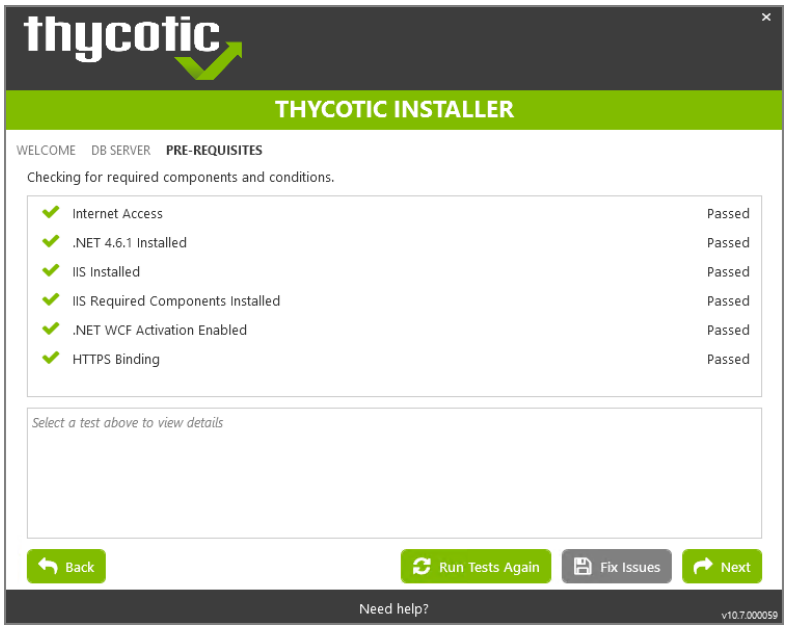
3. On the **Database** tab you can choose to either install SQL Express or connect to an existing SQL Server. SQL Express requires a internet access for the installer to download the installation package for SQL Express.



> **Note:** For production environments Delinea recommends installing a licensed edition of SQL before installing Delinea products. The Express edition is only recommended for trial and sandbox environments.

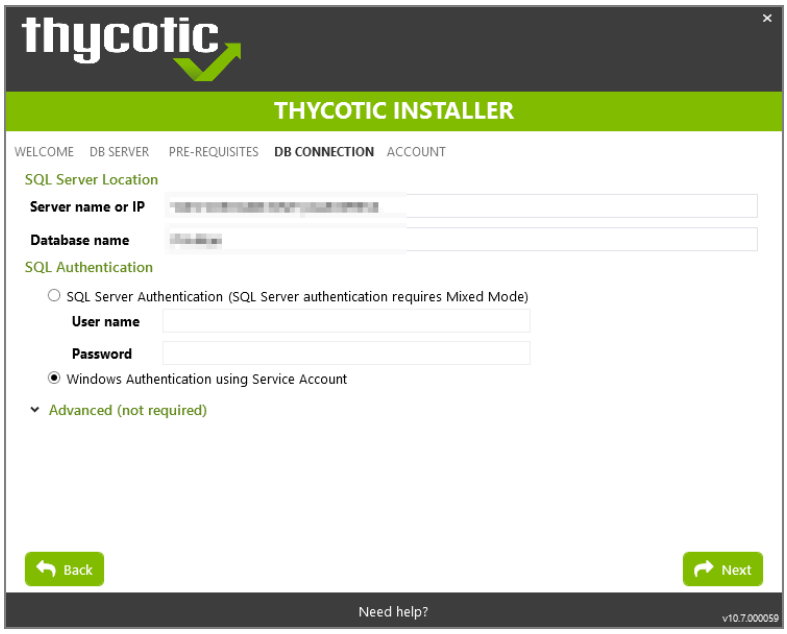
- If Internet access is not available a link to download SQL Server Express will be presented to the user. At that point, they are expected to install SQL Server Express and then restart the installer.
- If Internet Access is available SQL Server Express will be installed.
- After SQL is installed select Connect to an existing SQL Server.

4. The **Pre-Requisites** tab makes sure everything that is required to install Privilege Manager is setup correctly. Everything on this page can be installed outside of the installer, but if not, the installer will install and configure them for the user. Think of this page as the non-Delinea configuration. If there are issues with this page it is very likely that the Internet will be able to help as these are not installation features that are specific to Delinea. Click Fix Issues to automatically install the necessary pre-requisites. When Successful, click Next.



5. If you chose the "Connect to an existing SQL Server" option on the Database page, the **Database Connection** tab will now prompt you for the connection information that Privilege Manager will use. The Test Connection button must be run successfully before installation can continue. Once connection is established, click **Next**.

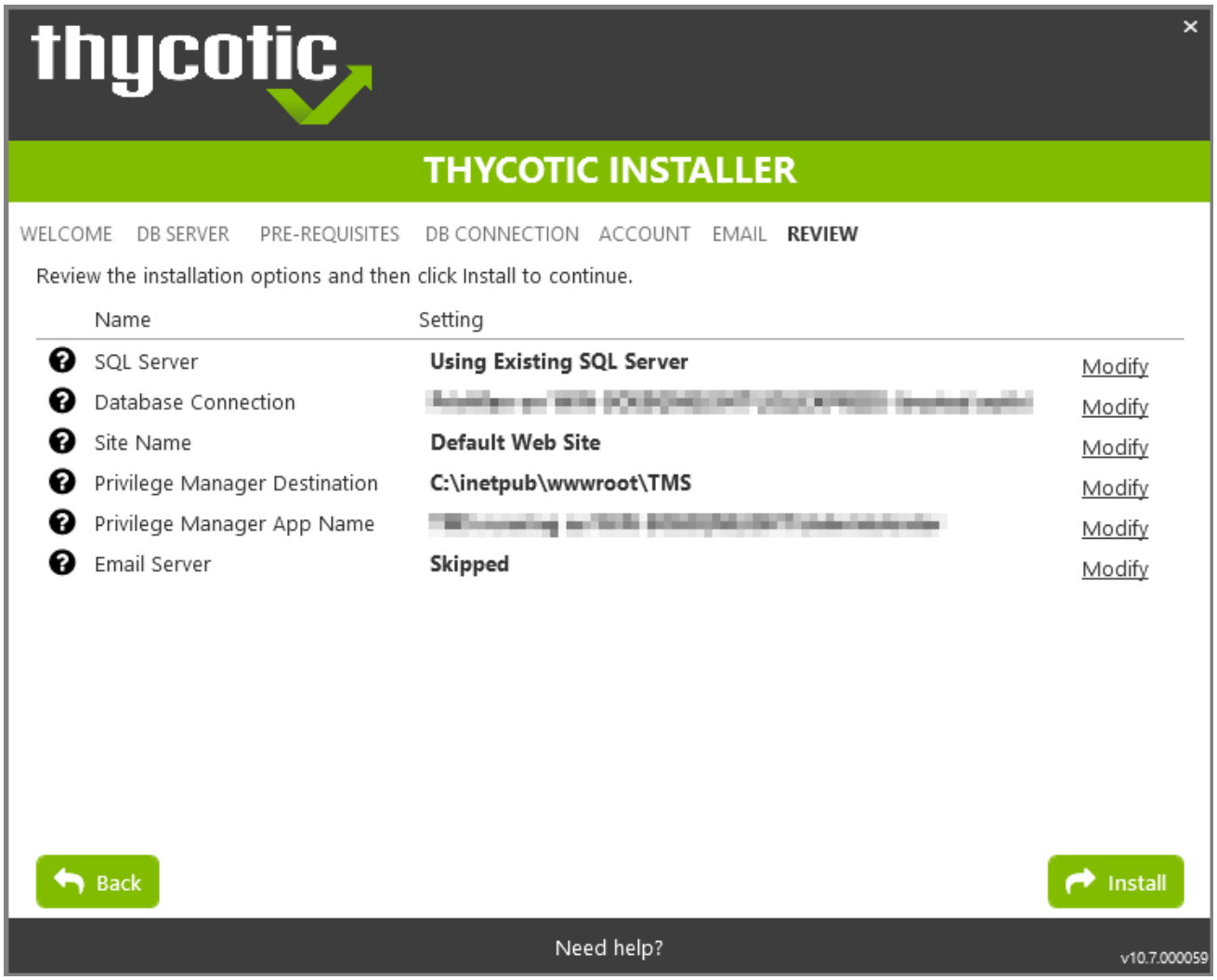
   Note: If you are not using a default InstanceName on the SQL Server for the Privilege Manager database, provide the SQLServerName\InstanceName for **ServerName or IP**.



a. If you choose SQL Server Authentication, next the Account tab will prompt for the server location where your SQL database is currently installed. Provide the Server Name or IP address for your Database server and Authenticate with Administrator SQL credentials. If your Secret Server database does not yet exist when you click "Test Connection" the Installer will create it. When the connection has been tested successfully, click Next.

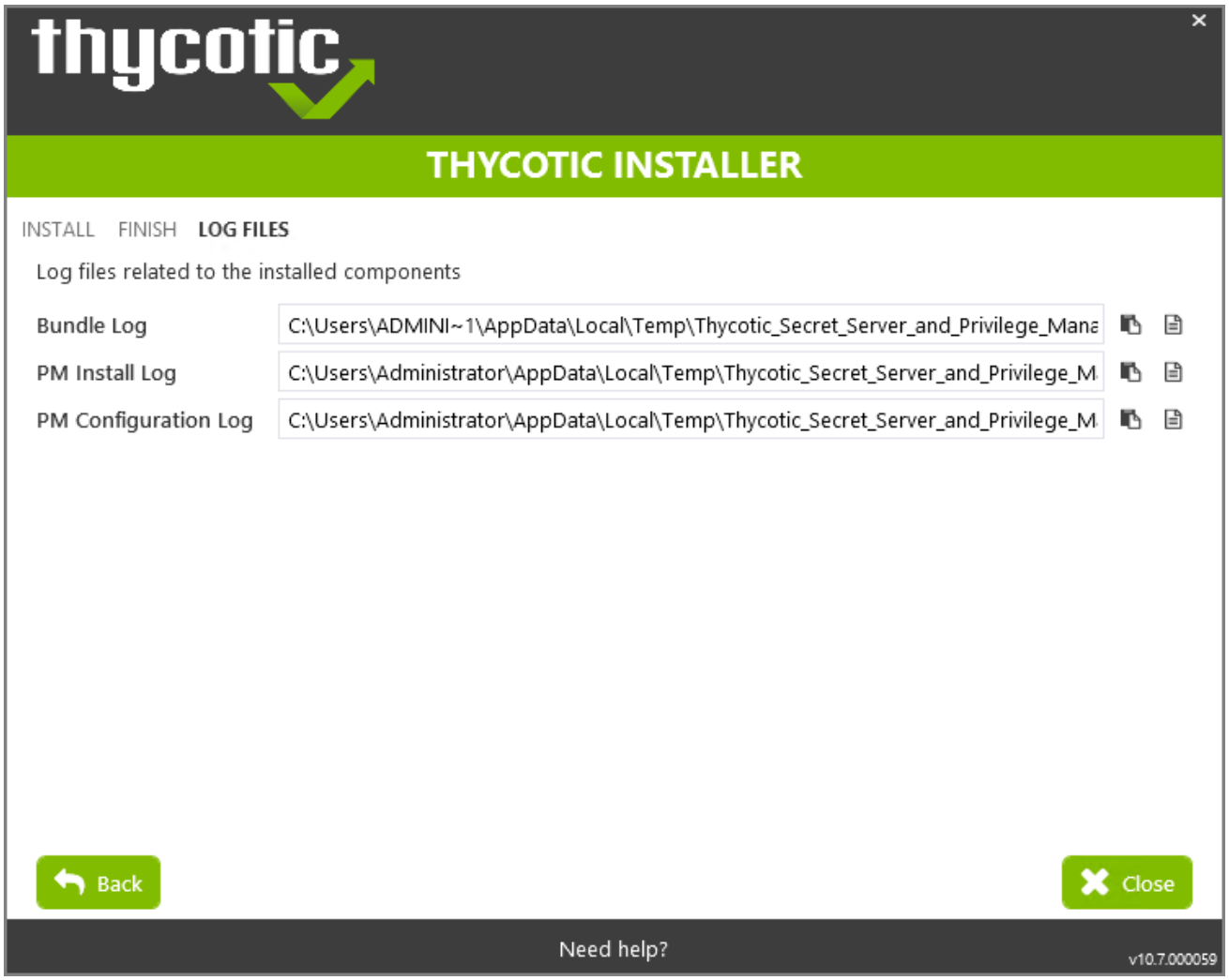
6. The **Email Server** tab opens, here the connection information for the email server can be entered. This is also optional and can be skipped to be configured later in the application by clicking Skip Email. This page will configure email for Privilege Manager.

7. On the **Review** tab, most settings are defaulted for a user and they can choose to modify settings at this step. Certain validations will occur on these settings before the install can begin. Click Install to proceed.

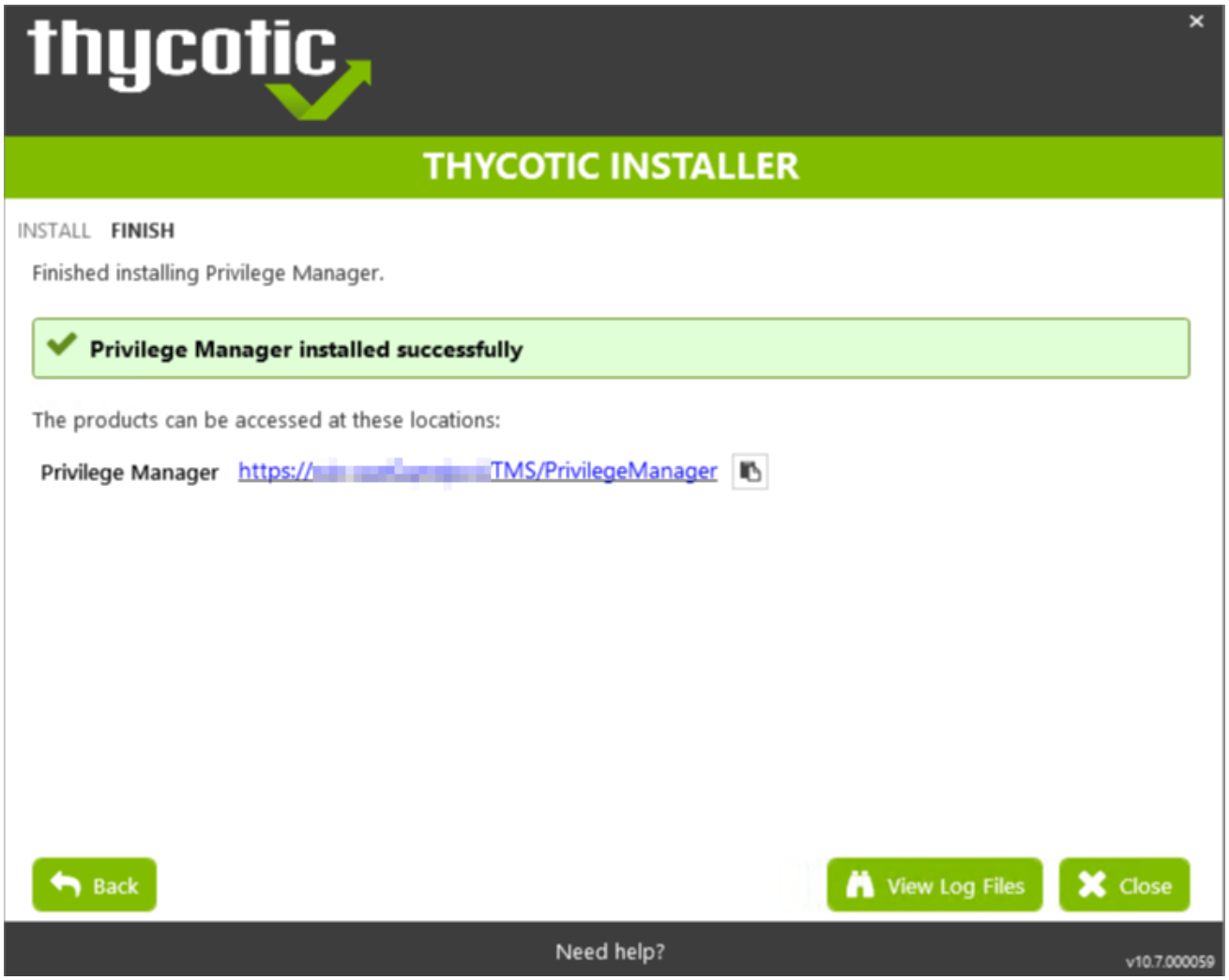


8. The Install page will show the status from log files as Secret Server and/or Privilege Manager are installed. Installs vary depending on your environment, most installs last between 20-60 minutes.

9. The **Log Files** tab is available after the applications are installed. The installer provides the link to open a web browser to the product login page. At this point, everything is installed and ready for you to begin using your new Delinea product. If the installation failed or you wish you view the logs from the installation you can click the View Log Files button.



10. On the **Finish** tab, when the install has successfully completed, click the provided Privilege Manager URL to navigate directly to your setup landing page or open a browser and navigate to where your Privilege Manager is located, for example: http://localhost/TMS/PrivilegeManager.



Note: Delinearecommends to create a back-up copy of the Privilege Manager web application folder after installation or upgrades.

Installing Connectors or the API

Privilege Manager installs the core packages. Once your instance is up and running, use Setup to add connectors for foreign systems or the **Privilege Manager Application Programming Interface**.

Refer to Upgrades for details about how to access Setup and use the **Add / Upgrade Privilege Manager Features** option.

Clustering Privilege Manager

To install Privilege Manager in a cluster, follow the steps above to install the application on the primary server. Then follow the Migration Steps to copy the web files to the secondary server and configure the secondary site. Then follow the steps for any additional servers in the cluster.

Manual Installation

If you need to manually install Privilege Manager on a system and you already have an existing server installation, refer to the installation instructions described under the High Availability Set-up for Privilege Manager. Otherwise follow the steps below.

Note: Delinea recommends to always use the setup.exe installer to verify that your system meets the prerequisites.

Download Privilege Manager Application Files

Make sure you have the prerequisites (IIS, .NET Framework, and SQL Server) installed before following the steps listed below.

After clicking the download link on the Software Downloads page, you will be able to download a .zip file that contains both Privilege Manager and Privilege Manager files.

Zip File Extraction Tool

You will also need to install a zip application like winzip or 7-zip to extract files for this install. 7-zip is used in the instructions below and can be downloaded for free here.

Manual Installation (no setup.exe)

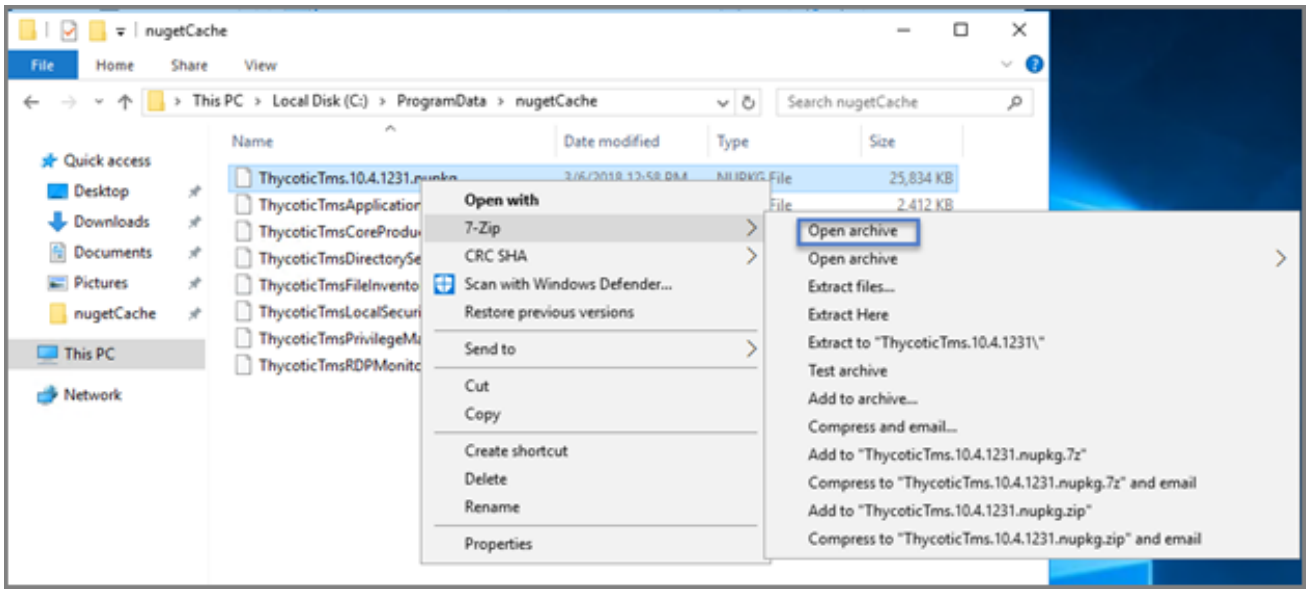
Clicking the download link above will take you to a portal page where you can choose to download a .zip file that contains the application files. Use this .zip file for the instructions below. Privilege Manger can be installed in a few different ways, as a:

- virtual Directory
- website

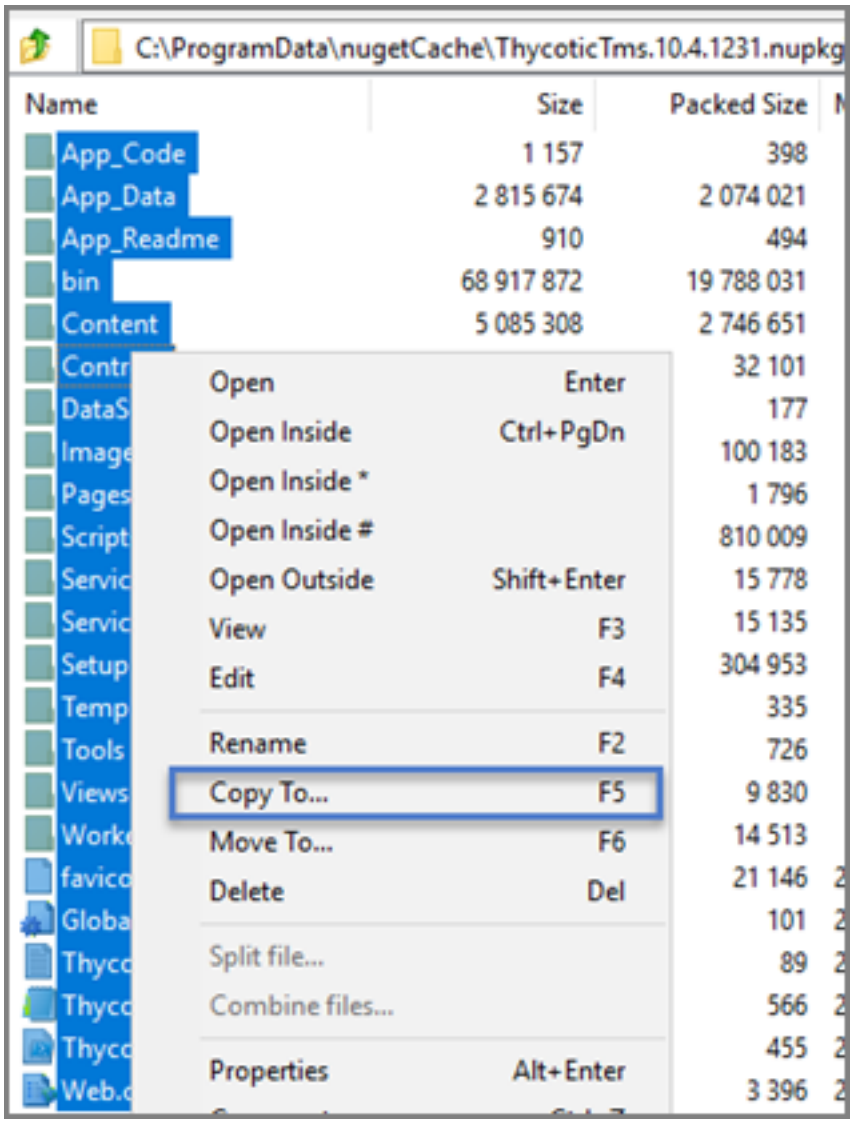
Installing as a Virtual Directory

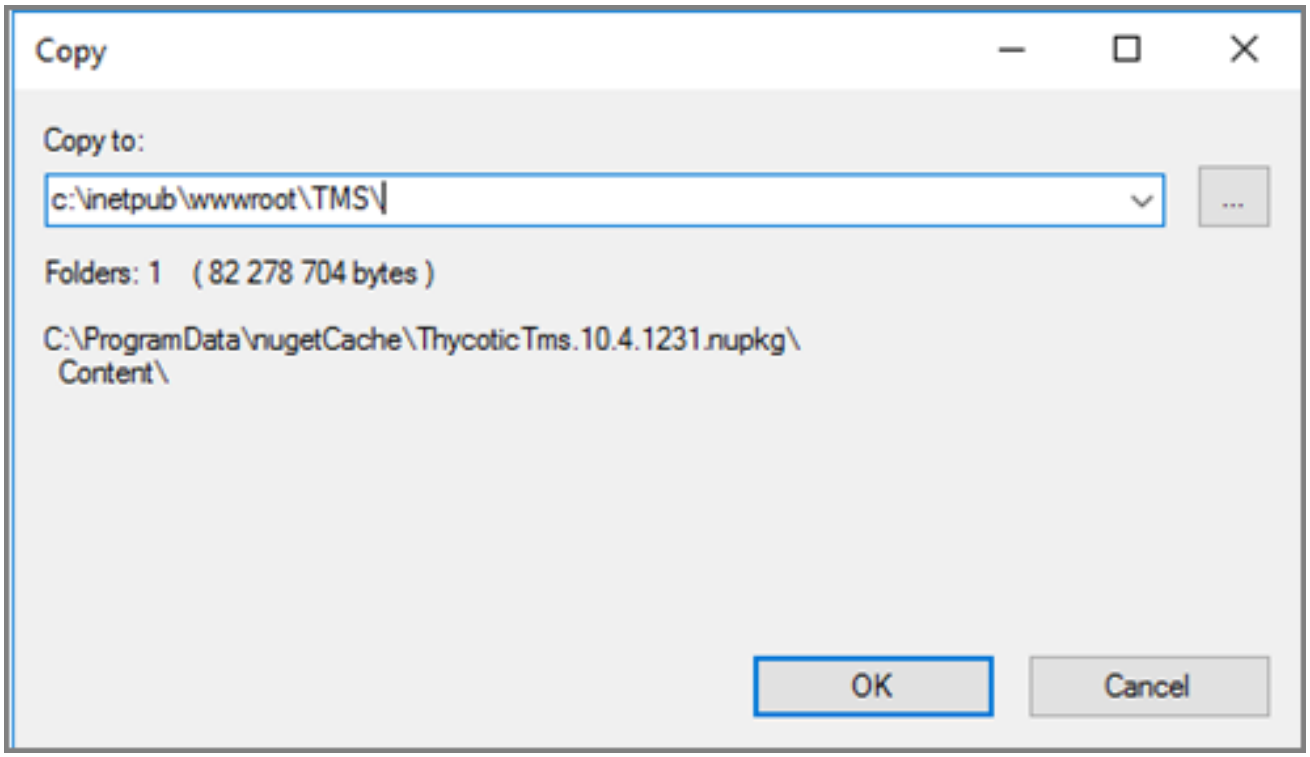
1. Extract the contents of the .zip file and select the nugetCache folder. Move the contents of that folder to a temporary location like `C:\ProgramData\` (Recommended)
2. Create a folder called TMS in the location `C:\inetpub\wwwroot\`
3. Navigate back to `C:\ProgramData\nugetCache\` and using any zip application (e.g., 7-zip, winzip, winrar), open `ThycoticTms.xx.x.xxxx.nupkg`

   To do this with 7-zip, right click `ThycoticTms.xx.x.xxxx.nupkg` and navigate to 7-zip | **Open Archive**.

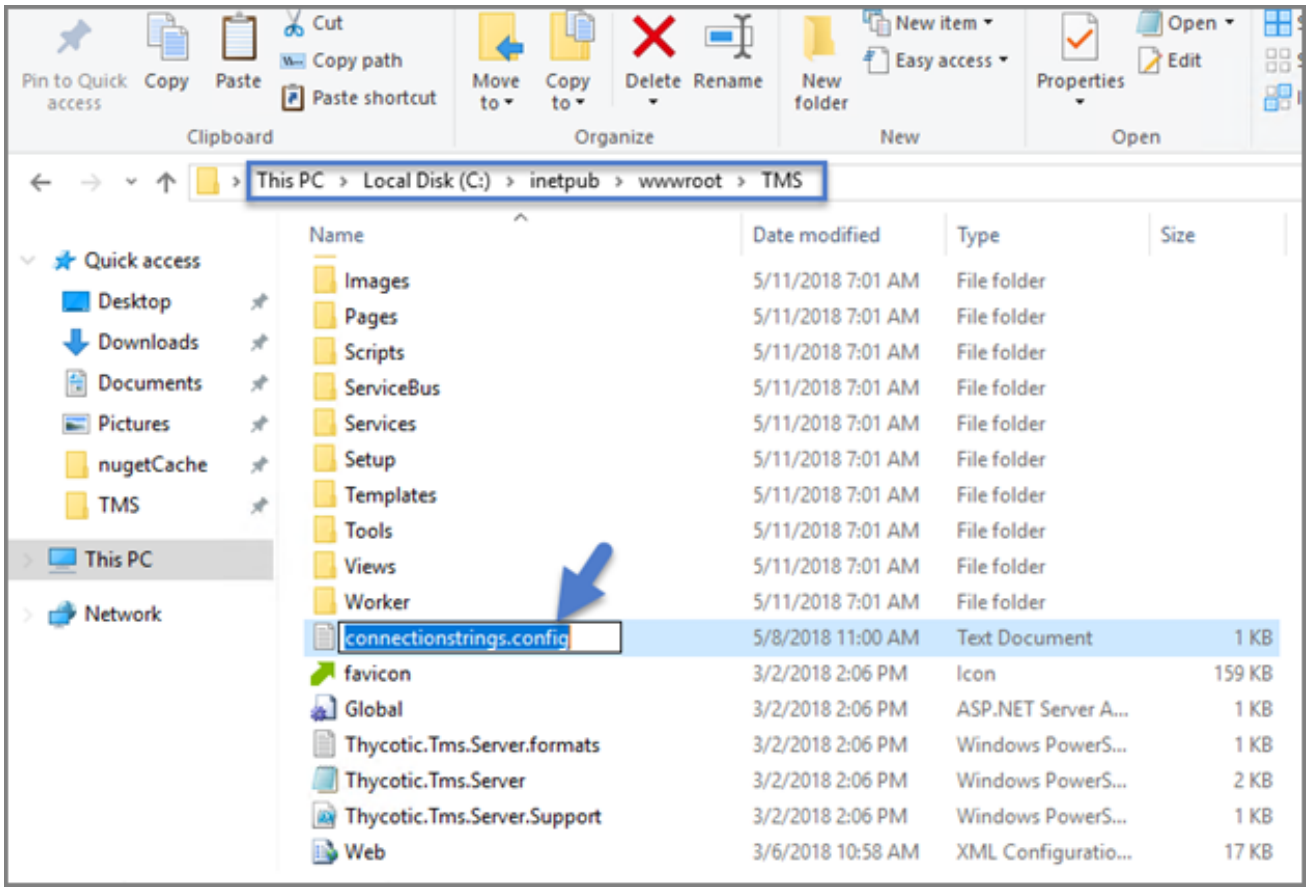


4. Open the Content directory and enter Ctrl-A to select all of its contents. Copy these to the location `C:\inetpub\wwwroot\TMS\`


C:\ProgramData\nugetCache\ThycoticTms.10.4.1231.nupkg
Name
Size
Packed Size
App_Code
App_Data
App_Readme
bin
Content
Open
Enter
Open Inside
Ctrl+PgDn
Open Inside *
Open Inside #
Open Outside
Shift+Enter
View
F3
Edit
F4
Rename
F2
Copy To...
F5
Move To...
F6
Delete
Del
Split file...
Combine files...
Properties
Alt+Enter



5. In `C:\inetpub\wwwroot\TMS\` where you have extracted the TMS Site files, create a new file and right click **New | Text Document** called `connectionstrings.config`



6. Next, decide what mode you want to use to access your SQL database and follow the corresponding steps:
   - **Mixed Mode/"Integrated Security=False"** (for easiest configuration): Mixed Mode is required if you intend on using a SQL Server account to authenticate Privilege Manager to your SQL Server instance. If you are doing an evaluation and using the Privilege Manager setup.exe installer, we recommend using Mixed Mode with a SQL authentication account. This option will also require you to set a password for the SQL Server system administrator (sa) account. See the Integrated Security=False section below to use Mixed Mode.
   - **Windows Authentication Mode/"Integrated Security=True"** (recommended for best security): This will prevent SQL Server account authentication and requires a Windows Service account to run the Privilege Manager website. This will also require additional configuration in IIS once Privilege Manager is installed. Follow the steps under the Integrated Security=True section below to use Windows Authentication.

Integrated Security=False

Open in Notepad the `connectionstrings.config` file created in step 5 and copy in the following text, replacing the SQL Server Name, Database Name, User Name, and Password (highlighted in bold below) with values for your environment. Save changes.

```
<connectionStrings>
            <add name="ApplicationServerWorkflowInstanceStoreConnectionString"
```

```
                connectionString="Data Source=SQLServerAddress;Initial
Catalog=DatabaseName;Integrated Security=False;User
ID=myUserName;Password=myPassword;Application Name='Arellia Management Server - WF'" />
            <add name="AmsConnectionString"
                connectionString="Data Source=SQLServerAddress;Initial
Catalog=DatabaseName;Integrated Security=False;User
ID=myUserName;Password=myPassword;Application Name='Arellia Management Server'" />
            </connectionStrings>
```

Integrated Security=True

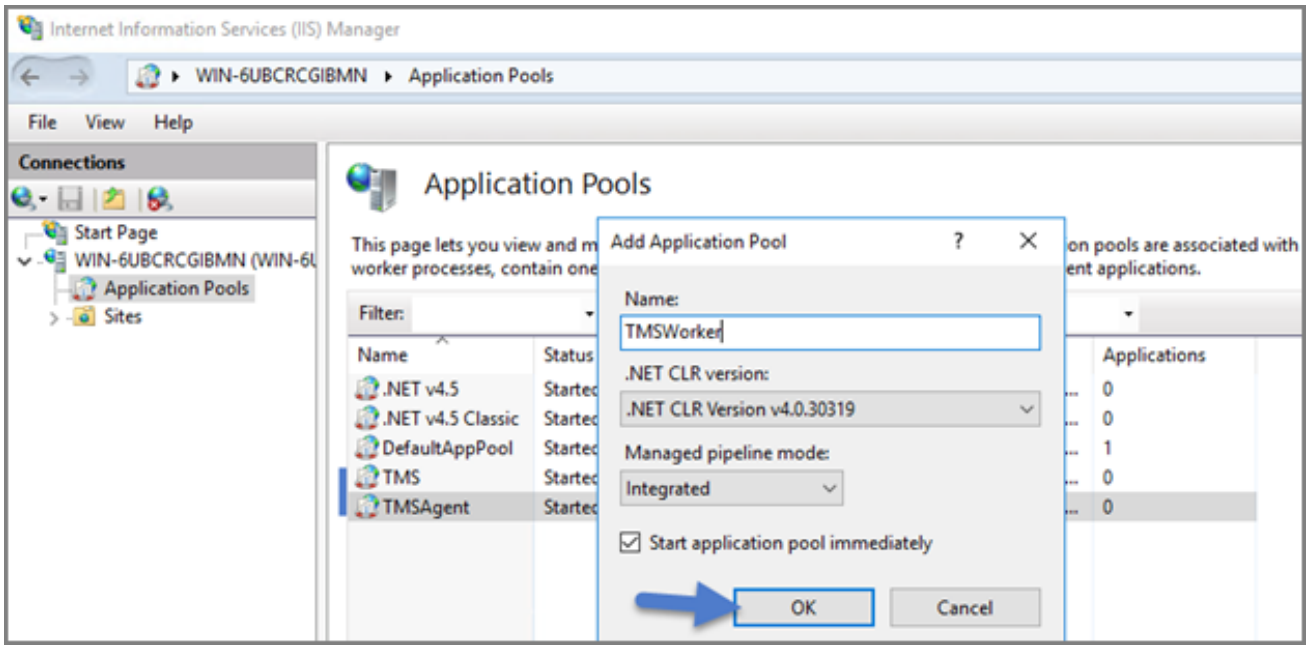
If you choose to set Integrated Security to True, you will need to ensure that the application pool service accounts have access to the database server in a later step.

Open in Notepad the `connectionstrings.config` file created in step 54 and copy in the following text, replacing the SQL Server Name and Database Name (highlighted in bold below) with values for your environment. Save changes.

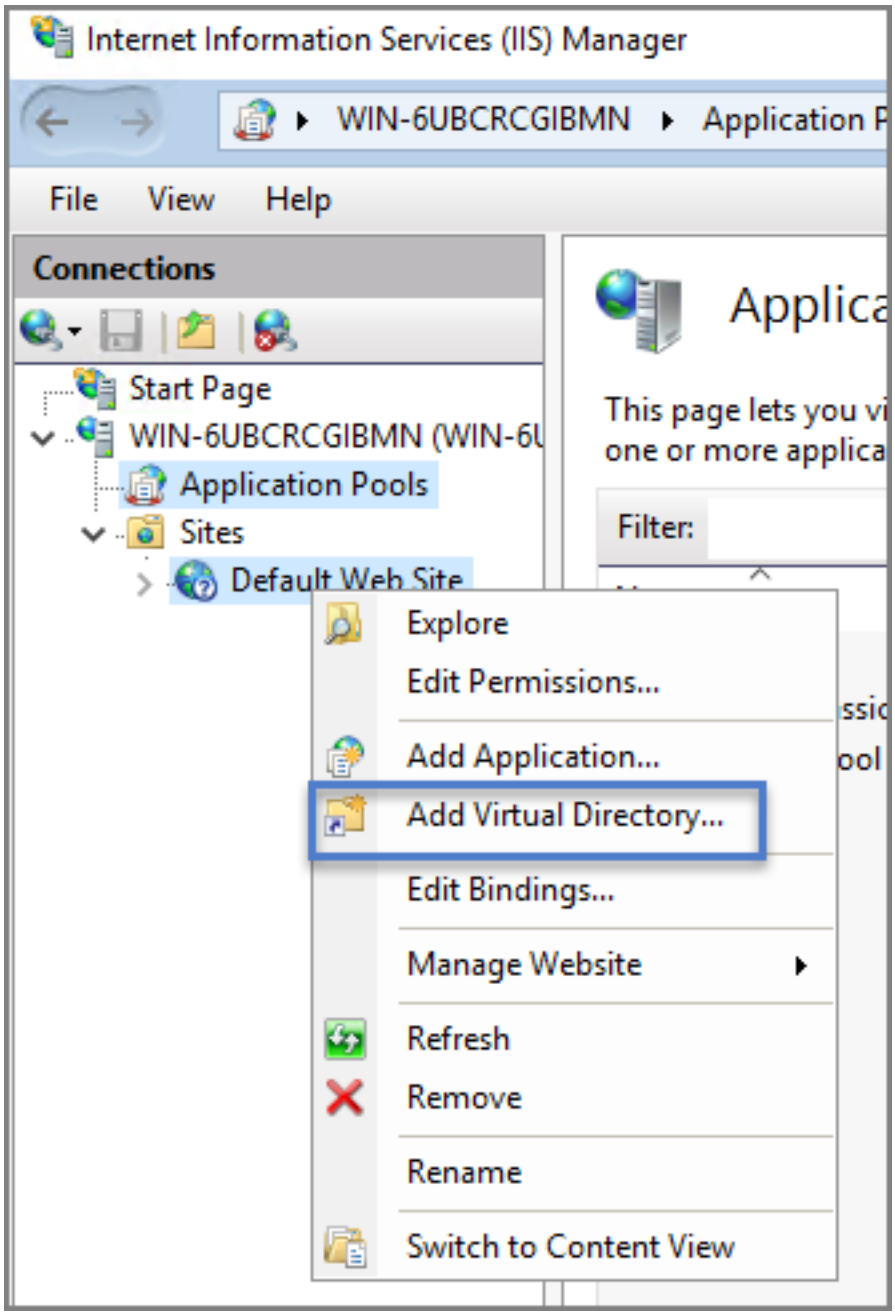
```
<connectionStrings>
            <add name="ApplicationServerWorkflowInstanceStoreConnectionString"
               connectionString="Data Source= SQLServerAddress;Initial Catalog=
DatabaseName;Integrated Security=True;Application Name='Arellia Management Server - WF'"
/>
            <add name="AmsConnectionString"
              connectionString="Data Source= SQLServerAddress;Initial Catalog=
DatabaseName;Integrated Security=True;Application Name='Arellia Management Server'" />
            </connectionStrings>
```

Continue: Installing as a Virtual Directory

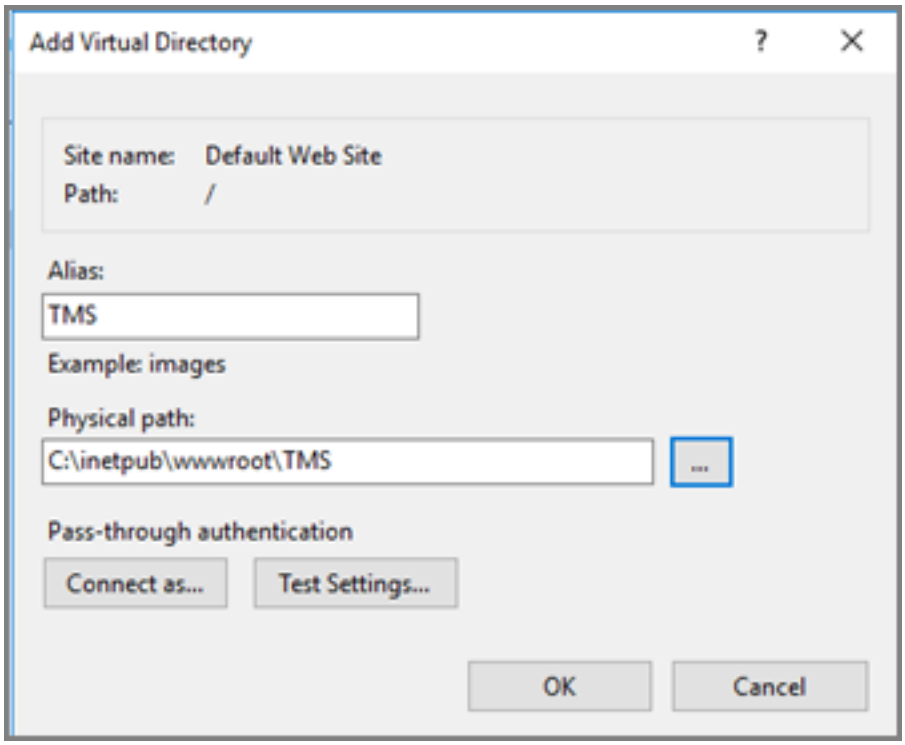
1. Open Internet Information Services Manager (InetMgr.exe).
2. Under your local server, right-click Application Pools and select **Add Application Pool...**. Add three new application pools. Name one "TMS," name another "TMSAgent," and name the third "TMSWorker."



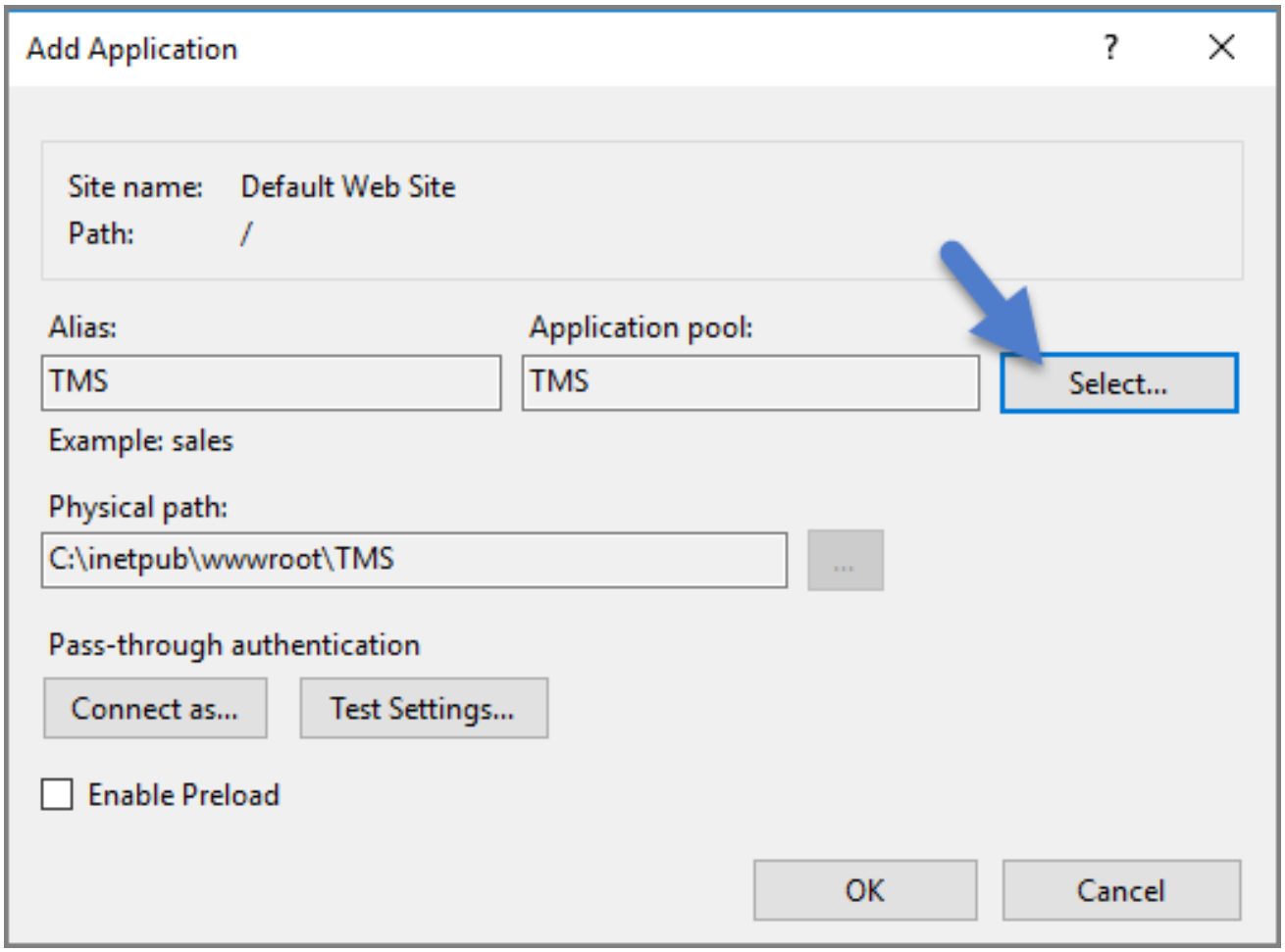
3. When creating your connection string, if you selected Integrated Security=True in step 6, change the Identity for your application pools to a service account that has DBOwner rights on the SQL database & make sure that the Identity for the three app pools have Modify rights to the folder that you put the Privilege Manager files into. To setup the service account correctly and set folder permissions and the Identities for these app pools, follow all of the steps in Using a Service Account to run the IIS App pool now.
4. Right click **Default Web Site** in IIS and select **Add Virtual Directory**.



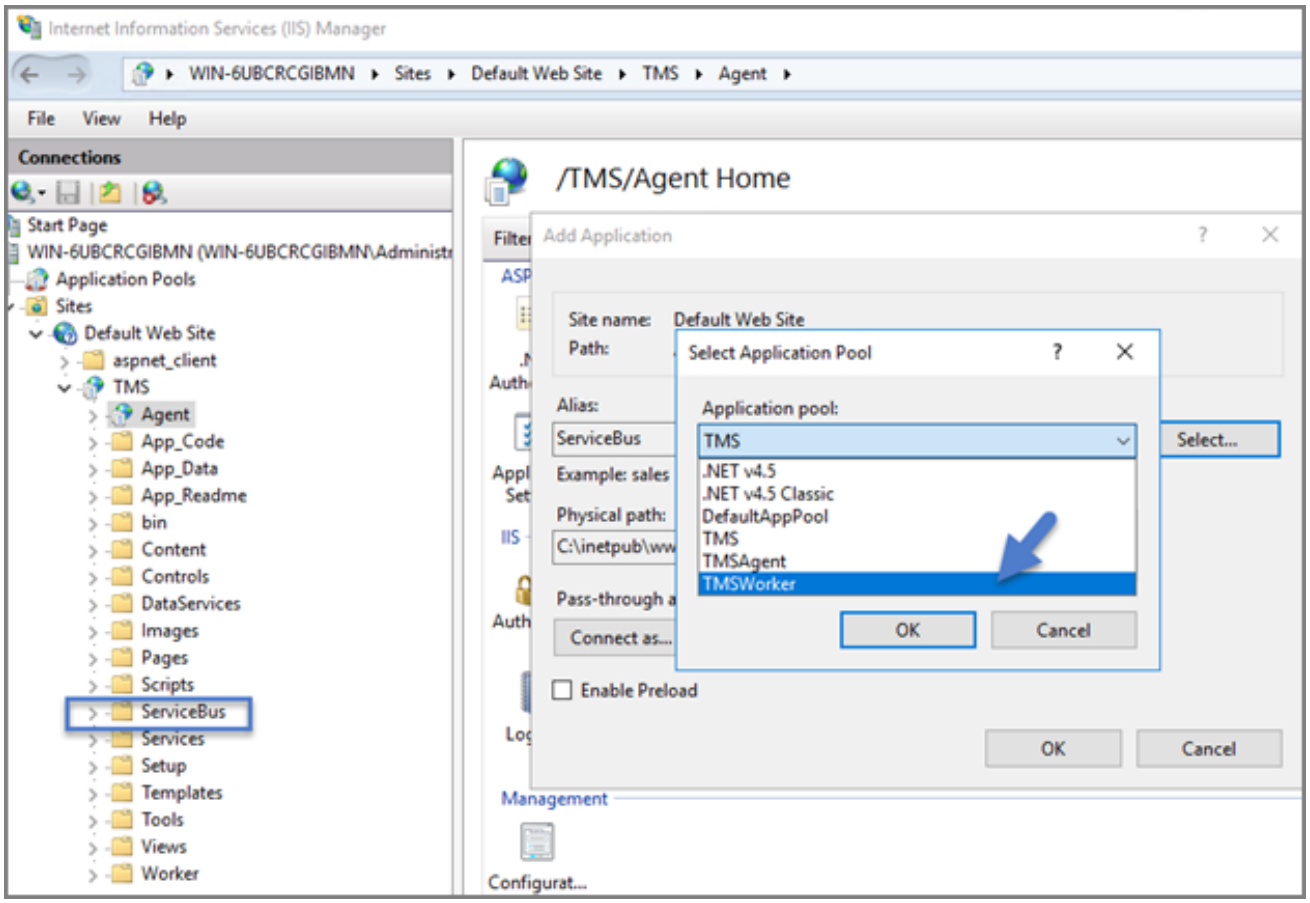
5. Select an alias for your Privilege Manager. The alias is what will be appended to the website. For instance, "TMS" in `http://myserver/TMS`.
6. Next, enter the physical directory where you unzipped Privilege Manager`C:\inetpub\wwwroot\TMS\`.
7. Click **OK**.



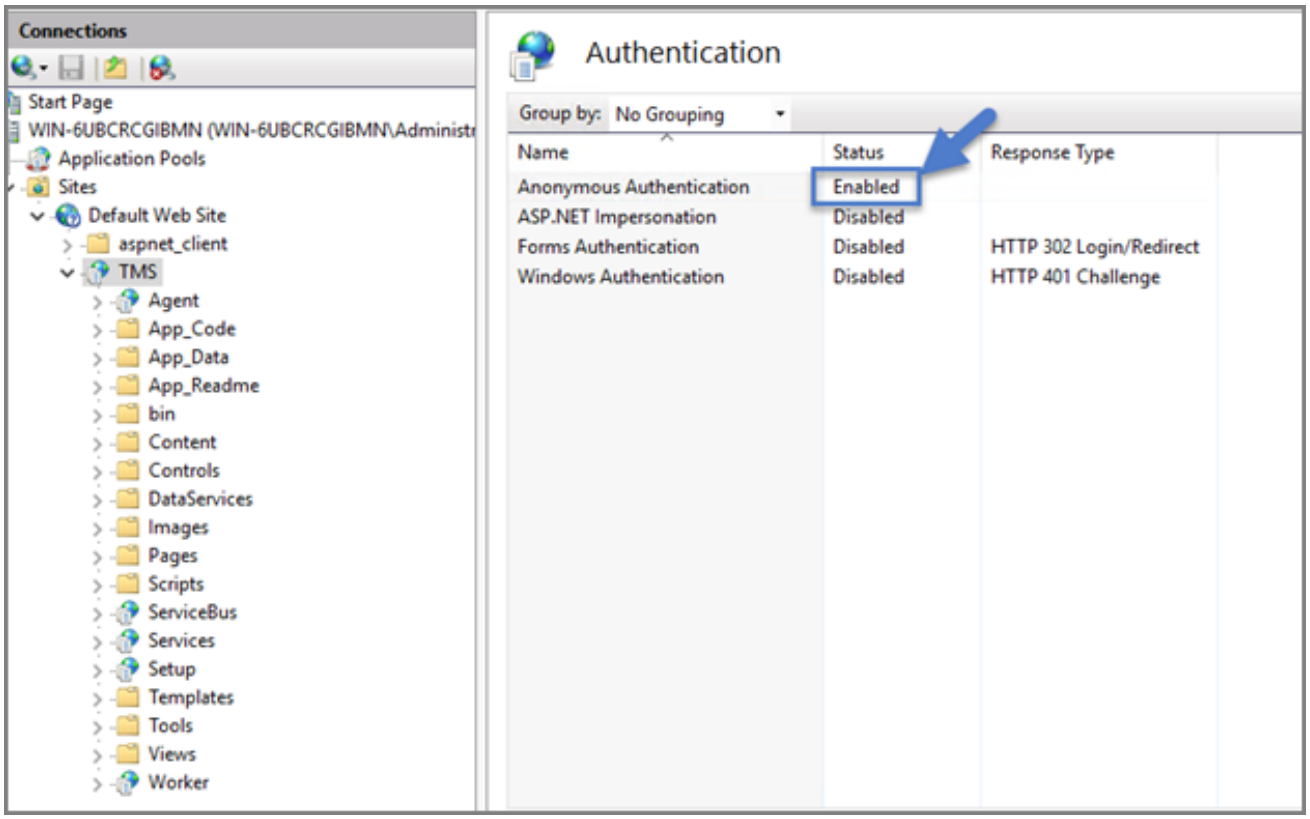
8. In the tree, right click the new virtual directory and select **Convert to Application**.
9. Set the **Application pool**l to the one called **TMS**. Click **OK**.



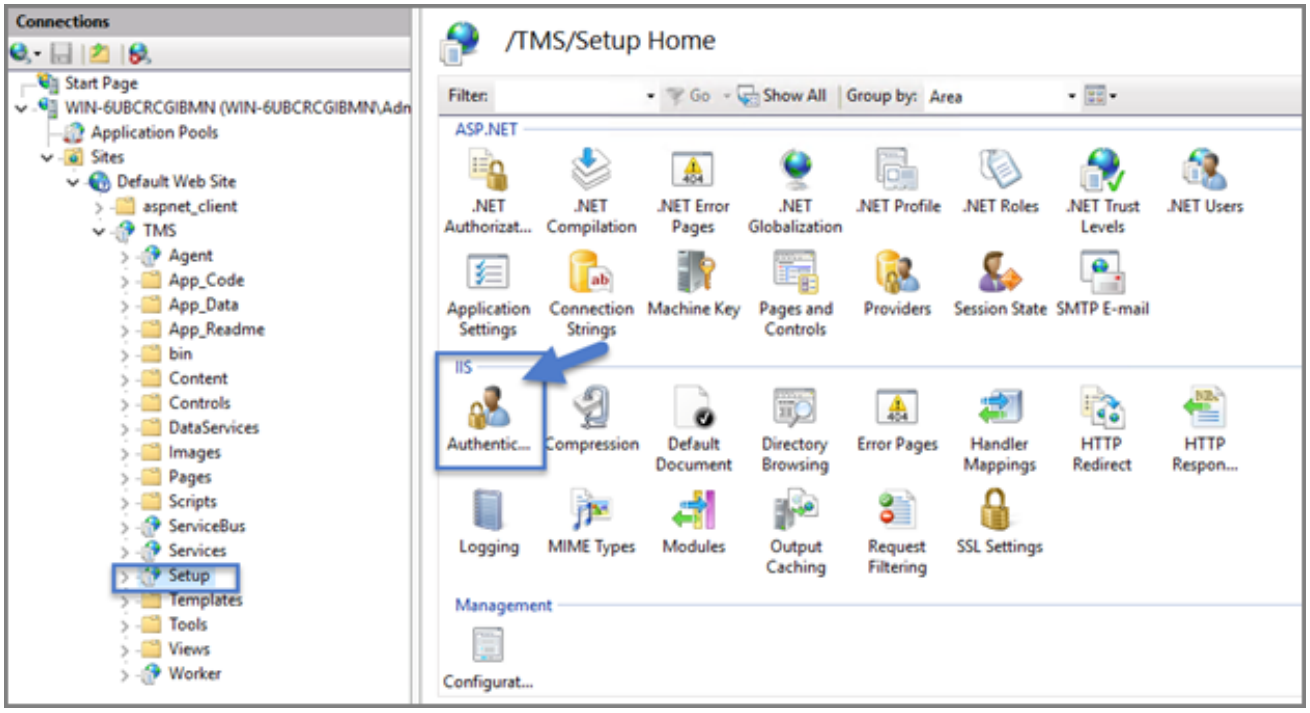
10. In the virtual directory expand the new TMS site, right click the **Agent** sub-folder and select **Convert to Application**.
11. Set the **Application pool**l to the one called **TMSAgent** and click **OK**.
12. Next, in the virtual directory navigate to the **ServiceBus** sub-folder. Right click and select **Convert to Application**.
13. Set the Application Pool to the one called **TMSWorke**r. Click **OK**.



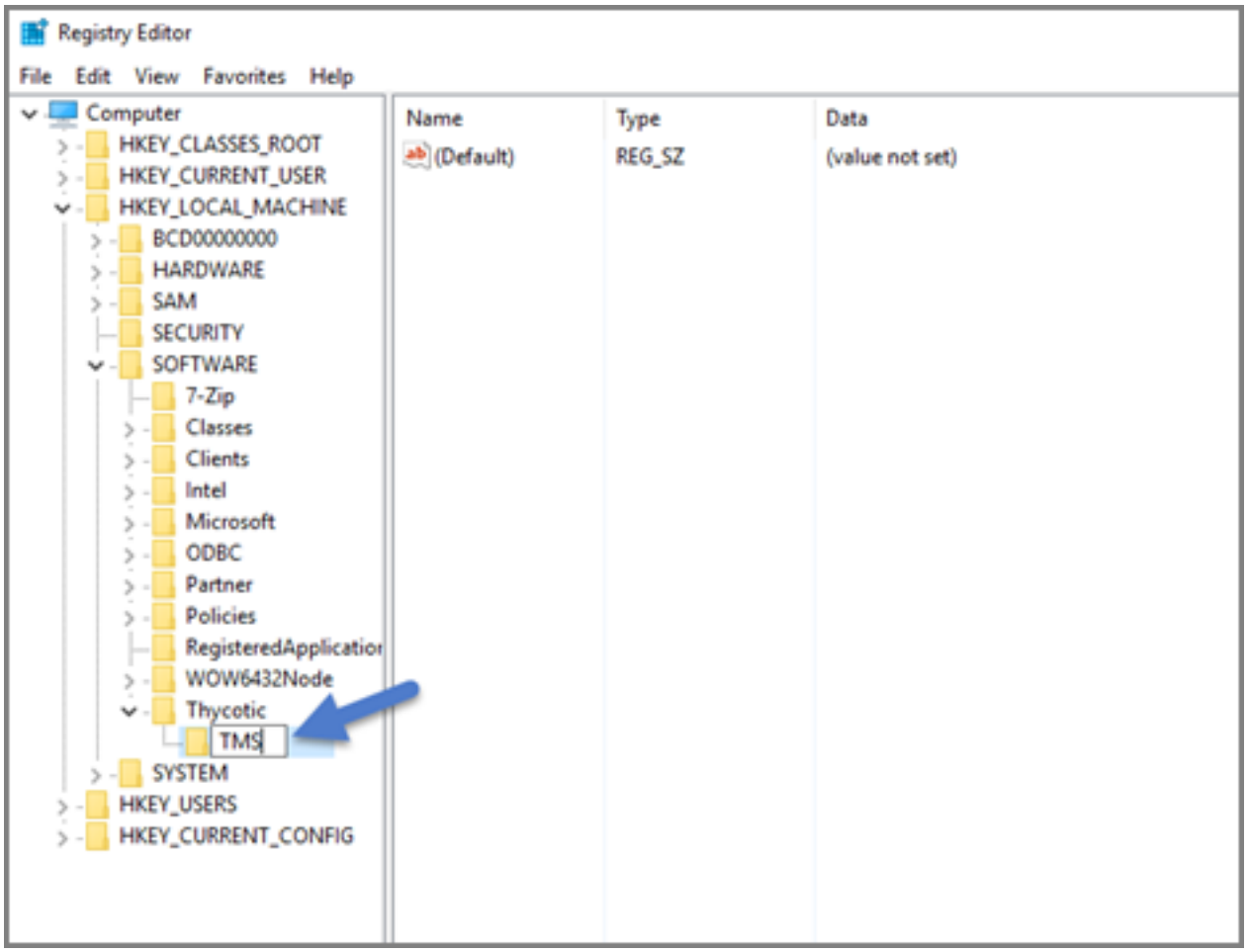
14. In the virtual directory, select the **Services** sub-folder, right click the new virtual directory and select **Convert to Application**. Ensure that the Application Pool is set to the one called **TMS**. Click **OK**.
15. In the virtual directory, select the **Setup** sub-folder, right click the new virtual directory and select **Convert to Application**. Ensure that the Application Pool is set to the one called **TMS**. Click **OK**.
16. In the virtual directory, select the **Worker** sub-folder, right click the new virtual directory and select **Convert to Application**. Set the Application Pool to the one called **TMSWorker**. Click **OK**.
17. Select your TMS virtual directory, double click **Authentication** in the features pane and make sure that only **Anonymous Authentication** is set to **Enabled**. Everything else should be set to disabled.



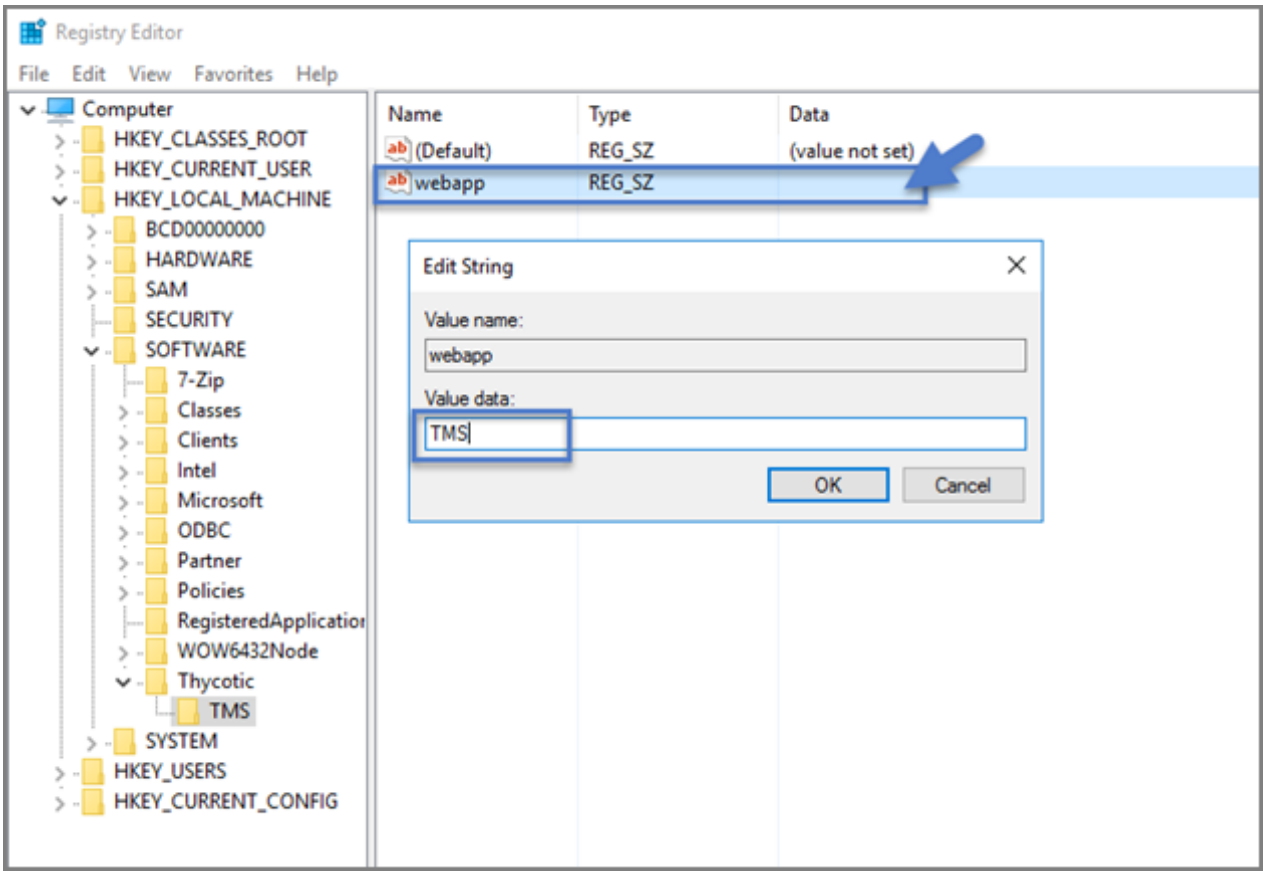
18. Select the **Setup** directory, double click **Authentication** in the features pane and make sure that **Anonymous Authentication** and **Windows Authentication** are both set to **Enabled**. Everything else is disabled.



19. Select the **Worker**, double click **Authentication** in the features pane and make sure that **Anonymous Authentication** and **Windows Authentication** are both set to **Enabled**. Everything else is disabled.
20. In **Regedit.exe**, create a new Registry key (HKEY_LOCAL-MACHINE\ right click on **Software | New | Key**, name the new key "Thycotic." Next, right click **Thycotic | New | Key** and name the new key "TMS."



a. Create a new string value in the TMS folder. Right-click **TMS | New | String Value** for webapp and a value of TMS (double click to assign value).



b. Create a second new string value with a name of the website and a value of the URL to the root of the site you will be using (i.e., "testlab" for a website of `https://testlab/TMS`)

c. Create a new string value with a name of "Webdir" and a value of the path you put your Privilege Manager files in (i.e., `C:\inetpub\wwwroot\TMS\`)

21. Ensure that the Privilege Manager folder has the proper permissions by checking that the account running the application pool in IIS has Modify permissions on the folder where Privilege Manager is installed. (i.e., C:\inetpub\wwwroot\ right click **TMS | Properties | Security** tab, if the service account created in Using a Service Account to run the IIS App pool is not listed, **Edit** | **Add** | find account via **Check Names** | **OK**. Click on the account, check **Modify | Apply**.)

22. If your server does not have internet access you will need to ensure that your **solutionCenter** is configured for the directory that you deposited the nupkg files into.

    a. Go to the directory where you have installed the TMS site (i.e., `C:\inetpub\wwwroot\TMS`)

    b. Open the **web.config** file with Notepad and find the line:

```
<add key="nuget:source:SolutionCentre" value="http://tmsnuget.thycotic.com"" /
```

    c. Replace the value with the directory from step 1 (usually `c:\ProgramData\NugetCache\`). Save changes.

```
    <add key="elmah.mvc.requiresAuthentication" value="false" />
    <add key="elmah.mvc.allowedRoles" value="*" />
    <add key="elmah.mvc.route" value="elmah" />
    <!--                <add key="nuget:source:DevSolutionCentre" value="http://localhost/TmsDevNuget/NuGet/"/>         <add
key="nuget:source:SolutionCentre" value="http://nuget-dev.ds.arellia.com/NuGet/"/>              <add
key="nuget:source:SolutionCentre" value="c:\programdata\nugetcache\" />-->
    <add key="nuget:source:SolutionCentre" value="c:\ProgramData\NugetCache\" />
  </appSettings>
  <connectionStrings configSource="ConnectionStrings.config" />
  <system.web>
```

Note: Make sure if using a local path to include the final slash.

Privilege Manager is now ready to be configured. Continue with Completing Privilege Manager Installation from the website.

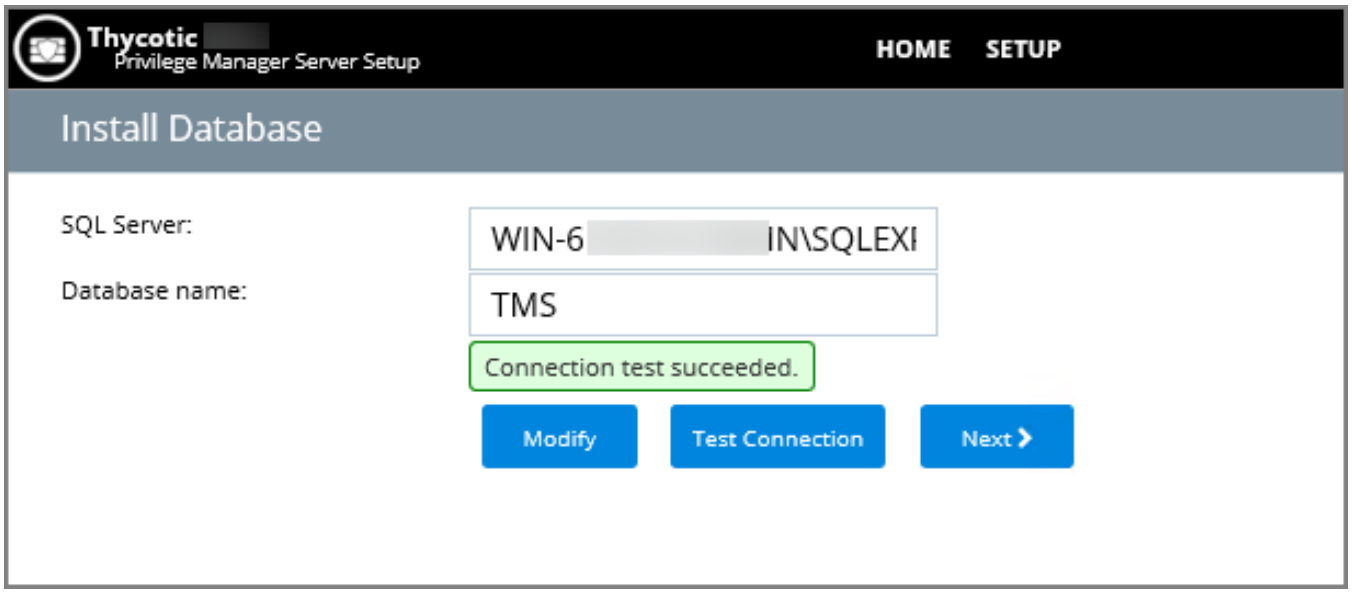
Installing as a Website

1. In IIS, right **Sites** and select **Add Website**.
2. Enter a **Site name**.
3. Click **Select** and choose the application pool you created in the Manual Installation section from the drop-down menu. Click **OK**.
4. Click the **...** beside the Physical path field and select the directory containing the unzipped Privilege Manager files (i.e., `C:\inetpub\wwwroot\TMS`). Click **OK**.
5. At the bottom of the Add Website window, click **OK** to save your settings.

Completing Privilege Manager Installation from Website

Privilege Manager is now ready to complete installation. Open a browser and navigate to where your Privilege Manager **Setup** is located, for example: `https://localhost/TMS/Setup`. It will request windows credentials which must be the credentials for a local administrator on the web server.

The site will detect that is does not have the proper database configuration and walk you through installing the initial database objects.



After this initial step, you will be presented with a list of Privilege Manager features you can choose to install.

1. Select **Add/Remove Product Features**.
2. Select **Application Control** and Privilege Manager. This will automatically also select any prerequisites they require.

   Each feature is delivered as a NuGet Package, the package will unzip, add files to the Privilege Manger website, and update the database with its required objects. Installing the database and features may take several minutes.
3. Click **Show Install Log** to reveal installation progress.

Once all features have been installed, Privilege Manager is ready to use! Refer to the Getting Started section for setup and configuration advice.

> **Note:** Delinea recommends to create a back-up copy of the Privilege Manager web application folder after installation or upgrades.

Considerations

The following guidelines that affect installation should be considered.

- "Package Hash Verification" on page 59
- "Item Encryption" on page 59
- "Antivirus Exclusions" below

Antivirus Exclusions

For Privilege Manager users, we recommend several anti-virus exclusions to maintain application performance and integrity. These guidelines apply to both real time and on-demand antivirus scanning.

Directories

Exclude these directories from your antivirus filters to ensure Privilege Manager processes will not be blocked (or for a more granular approach to these exclusions, see the Client Item Database and Privilege Manager Application Control Agent Services sections at the end of this article):

```
%ProgramData%\Arellia\
%ProgramData%\Application Data\Arellia
%ProgramFiles%\Thycotic\
```

Exclusions for Web Server

Exclude the following antivirus programs for Privilege Manager's web server, also sometimes TMS:

Temporary ASP.NET Files

Exclude the following directory to prevent degradation in performance and possible unexpected restarts of the Tms and TmsWorker IIS application pools:

`%SYSTEMROOT%\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files`

Exclusions for Database Server

Exclude the following database files.

SQL Server Data Files

These files contain data and typically have the following extensions:

- .mdf - primary data filegroups
- .ndf - secondary data filegroups
- .ldf - transaction log filegroups

SQL Server Backup Files

These files contain the backup files and typically have the following extensions:

- .bak - database backup files
- .trn - transaction log backup files

By default, the directories that contain the Data and Backup files are located under `C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL`.

SQL profiler trace files

These files contain SQL Profiler Trace log data and can be contained in any folder.

They usually have the file extension .trc.

Exclusions for Managed Workstations

Windows Agents

Exclude the following for managed workstations.

Request Run As Administrator Registry Key

Privilege Manager Application Control installs a context menu item that allows executables to be "Request Run as Administrator."

This context menu is added under the following registry key which some antivirus programs incorrectly flag as malware:

`HKLM\SOFTWARE\Classes\exefile\Shell`

Client Item Database

These directories contain the Delinea Agent client item database and should be excluded from antivirus to prevent corruption:

- `%ProgramData%\Arellia\ClientItems`
- `%ProgramData%\Application Data\Arellia`

If required, you can further limit this exclusion to all files with the .db and .db-* extensions under this location.

Privilege Manager Application Control Agent Service

Some antivirus products require that the Privilege Manager Application Control service be excluded from tamper protection rules because Application Control manipulates other applications which antivirus products may mistake as malicious.

`C:\Program Files\Thycotic\Agents\ApplicationControl\ArelliaACSvc.exe`

macOS Agents

Depending on which version of the macOS agent is used, different directories can be excluded.

macOS Agent, version 11.3.3.1 and later

Exclude these directories from your antivirus filters to ensure Privilege Manager processes will not be blocked:

`/Library/Application Support/Delinea/Agent/usr/local/delinea/quarantine` (if the quarantine feature is being used)

macOS Agent before version 11.3.3

For older versions of the agent, these directories should be excluded:

`/Library/Application Support/Thycotic/Agent/usr/local/thycotic/agent/usr/local/thycotic/quarantine` (if the quarantine feature is being used)

Item Encryption

With version 10.5 and up, encryption of items no longer requires app pool permissions on the machine's certificate store.

What this means for Privilege Manager

New installations of Privilege Manager will no longer require that the application pool user has to have permission to access the certificate stores. Previously this permission was required in order to encrypt and decrypt items in the database.

Existing installs of Privilege Manager (10.4 and earlier) should not remove this permission and should not remove old certificates as they will still need them to decrypt old items which predate this change. Both the web setup page and the installers will create a local **encryption.config** file in the TMS directory to hold the keys to the key stored in the database. This file is highly sensitive and should be regarded with caution.

Package Hash Verification

Automatically when Online

Privilege Manager verifies the SHA512 hash of downloaded packages during the install/update process. Installation of packages does not happen if a downloaded package hash does not match with the NuGet server information.

The following measures are implemented:

- Privilege Manager prevents zero byte files from passing hash validation.
- Through hash validation, Privilege Manager ensures any download or disk write failures (disk space issues, rights, etc) do not leave remnants of partially extracted packages on the system.
- Privilege Manager writes a warning into the logs and does not start an install/upgrade from the install pages unless it can validate the packages. It re-checks when the install is running, to accommodate other Privilege Manager servers in a multi-server environment, so that each server checks packages while doing its install.

Tempering or disk-write failures are logged, those can be due to skipped package validation, when the hash cannot be received from the NuGet server, or for offline updates or packages that are considered pre-release and not yet publicly available. Also, files shares can be setup, restricting a user's write access to prevent tempering of downloaded packages, which is a best practice for offline environments.

> **Note:** For offline package installs, Privilege Manager assumes the user has validated the package integrity. Refer to **Validating Package Integrity for Offline Upgrades** below.

Validating Package Integrity for Offline Upgrades

Privilege Manager does not verify package integrity in offline scenarios without the following user action. Users need to either

- copy the package hash files along with the NuGet packages, or
- calculate the hash files themselves (see PowerShell examples below.

If a hash file isn't provided, integrity won't be validated and a warning will be logged.

Locally on your system, set the NuGet repository URL in the `web.config` file to the local repo address at `c:\ProgramData\NuGetCache`. Privilege Manager checks each file to see if there is a corresponding file with `.hash.json` extension. This json file contains the HashBase64 and HashAlgorithm property value pairs to verify integrity.

Example from `ThycoticTmsCoreProduct11.0.1035.nupkg.hash.json`:

```
      { "HashBase64":
"CXs8cQ+65r6YWPpfylQVWdE4jHD3BhkJHlnWykAx1iItpcKmYhx6mkof/haChlu6aH8M+gYXUEN2ErH8wOPPlg==",
"HashAlgorithm": "SHA512" }
```

Sample PowerShell script to calculate the hash for a package:

```
      $fileName = 'C:\ProgramData\NugetCache\ThycoticTmsCoreProduct.11.0.1040.nupkg'

$content = [System.IO.File]::ReadAllBytes($fileName)

$sha = [System.Security.Cryptography.SHA512]::Create()
$hash = $sha.ComputeHash($content)
$sha.Dispose()

$hashBase64 = [System.Convert]::ToBase64String($hash)

$hashBase64
```

Sample PowerShell script to take the NuGet package path and write an updated hash file:

```
      #
# Usage: UpdateNuGetHash.ps1 -NuGetFileName
C:\ProgramData\NuGetCache\ThycoticTmsCoreProduct.11.0.1040.nupkg
#
param([Parameter(Mandatory=$true)][string]$NuGetFileName)

$content = [System.IO.File]::ReadAllBytes($NuGetFileName)

$sha = [System.Security.Cryptography.SHA512]::Create()
$hash = $sha.ComputeHash($content)
$sha.Dispose()

$hashBase64 = [System.Convert]::ToBase64String($hash)

$hashFileName = "$($NuGetFileName).hash.json"$hashFileContent = "{ ""HashBase64"":
""$($hashBase64)"", ""HashAlgorithm"": ""SHA512"" }"[System.IO.File]::WriteAllText
($hashFileName, $hashFileContent, [System.Text.Encoding]::ASCII)

Write-Host "Updated hash file ""$($hashFileName)"" for nuget package ""$($NuGetFileName)""."
```

Unix/Linux Signature Verification

Customers can verify Signatures via detached signature verification, which requires three things:

- **FILE** - The original distributed file in which a signature file was derived
- **SIGNATURE** - The signature file derived from the distributed file ()
- **PUBKEY** - The public key file (cert) counterpart to the private key that was used to sign.

After issuing the following commands, a successful signature will result in **Verified OK**:

```
      $ openssl base64 -d -in <SIGNATURE> -out /tmp/sign.sha256
$ openssl dgst -sha256 -verify <PUBKEY> -signature /tmp/sign.sha256 <FILE>Verified OK
```

Note: OpenSSL v1.0.1 (or newer) is a required dependency PMAUL package signature verification.

Agent Installation

Agents are required on endpoint machines to carry out policies created in Privilege Manager. This section offers direct downloads and descriptions for all available agents.

Important: Before performing a new first-time installation of agent version 11.4.2 or newer, review the information presented in "Virtual Service Accounts" on page 90 completely and ensure that your runtime environment complies with the stated requirements. Failing to do so will result in the application control service failing to function properly.

Delinea Agents can be deployed in various ways, via:

- software management systems,
- GPO,
- cloned (gold) images, and
- manually.

Instructions and links for agent installers are grouped as follows:

Note: If you are using the Bundled Privilege Manager Agent Installer after previously using manual installers, the bundled installer will appear as the most recently installed file. For historical purposes, the manual installers will also appear.

- Windows Agents
  - Bundled Agent Installer - Windows
  - Individual Agent Installers for Privilege Manager:
    - 64-bit Windows Operating Systems
    - 32-bit Windows Operating Systems
  - Directory Services Agent to support Local AD Synchronization with Cloud Instances
  - Bundled Core and Directory Services Agents
- macOS Agent Installer - 10.11 or Newer

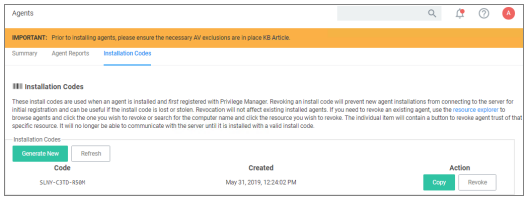
For details about Delinea Agent System Requirements, see the information provided for each agent OS introduction topic.

Agent Install Codes

In version 10.5 and up, installation codes are required upon initial install to prove to the server that an agent install is authorized. Once an agent is installed, it deletes the install code and authenticates to the server via a certificate. See Agent Trust Revocation for certificate revocation.

The agent uses the install code to prove to the server that it is an authorized install. Once the agent is installed, the install code is deleted and the agent certificate is used to communicate with the server. The server needs either an install code or agent trust (a certificate) to accept communication from an agent. Multiple install codes can be created for bundling with different installers, if the last install code is revoked, a new one is generated automatically. Revoking an install code prevents new installations with that install code but does not affect previous installations since those agents now use their own certificates to authenticate.

1. Navigate to the agent settings under **Admin | Agents**.
2. On the Installation Codes tab you may Generate New codes, Refresh code information, Revoke, or Copy Codes to the clipboard to use in the installer.



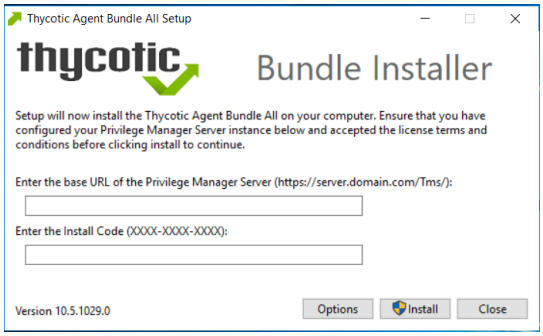
If deploying with msiexec, the following command shows an example for how to set the Install Code:

```
msiexec.exe /i ThycoticTmsSetup_x64.msi INSTALLCODE=1234XXXXABCD
AMSURL=https://DOMAIN/Name/
```

Where:

- ThycoticTmsSetup_x64 is the install file used.
- INSTALLCODE is argument taking the install code value.
- AMSURL is the argument taking the base URL to the TMS installation.

If installing via a bundled installer, the install code is placed in the **Enter the Install Code** field (dashes in the install code are for readability and are optional).



Using the SetAMSServer.ps1 Script

If it becomes necessary to set the install code after the agent is installed, an install code can be set using a PowerShell script that must be run as an Administrator. This script, along with other useful agent scripts, will be

located in the `C:\Program Files\Thycotic\Powershell\Arellia.Agent` folder on any machine with the Delinea agent installed and it is called **SetAMSServer.ps1**.

The script will request parameters, as follows:

- The first parameter the script will request is the URL of the server you wish to connect to; its value should be `https://PrivilegeManagerURL/TMS/`.
- The second parameter it will ask for is the install code.

Agents can be installed without an install code, but they will be unable to register with the server until an installcode is provided.

If older agents are used, the **Prevent Legacy Agent Registration (10.4 and older)** option might be checked in the **General** section under the **Admin | Configuration | Advanced** tab, which prevents older agents without install code from registering.

If an agent was previously installed and never revoked, the endpoint continues to have a valid certificate and a new agent can be installed with post-install registration.

Ports/Agent Access Information

- **Outbound (port 443 - HTTPS)**: This is the default access port through which the agent connects to the server. You may specify a different port based on your environment.
- **Inbound (port 5593)**: The is the default and only port that the agent listens on. This port is not required and you can block port 5593. If you block the port, the agents pull updates from the server based on a set schedule.
- **SQL (port 1433)**: This is the default SQL DB port. The SQL port can be customized.

Installing macOS Agents

The macOS agent package .pkg installer and uninstaller package .pkg is delivered as a .dmg file. You can use the installer directly on individual endpoints for testing or for production environments.

Starting with Privilege Manager v11, the agent implements a system extension (SYSEX) to support macOS versions Catalina and higher. If you need to support older versions of macOS that do not support system extensions, refer to the 10.8.2 documentation for installation instruction for the **KEXT** based agent.

For details about differences regarding KEXT and SYSEX versions, refer to macOS Extensions.

Refer to the Software Downloads for the current versions available.

Agent Components

The agent is made up of several components:

- Privilege Manager.app
- System Extension
- Preference Pane
- sudo Plugin
- Service Agent

macOS Agent System Requirements

Privilege ManagerVersion	macOS Version	System Extension	Kernel Extension
10.8 and earlier	10.11 - 10.15	N	Y
11.0 and later	10.15 and later	Y	N

Installing macOS Agents

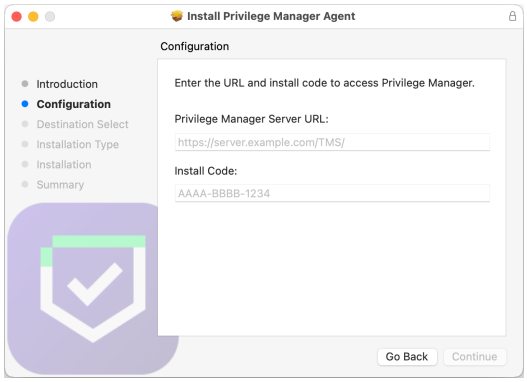
> Examples below are using version placeholders instead of the actual install package versions. If you copy the example, make sure to switch n.n.nnnn with the actual version numbers as listed on the Software Downloads page.
> If you enter the wrong install code or you need to update an install code for whatever reason, rerun the package installer to provide the correct/new install code. The Install Code field can be left blank when using versions lower than 10.5.

Directly

You can use the macOS agent installer directly on individual endpoints for testing or production environments.

To install the agent software on a single endpoint, follow these steps:

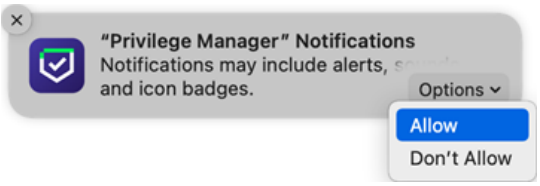
1. Go to Software Downloads - macOS Endpoints to download the Privilege Manager macOS Agent.
2. Mount the DMG and run the PKG installer on the computer you want to manage.
3. During the installation process,
   a. Enter the Privilege ManagerServer URL.
   b. Enter the install code.



If you are not using Mobile Device Management (MDM) to manage allowed system extensions, you will see the following dialogs.

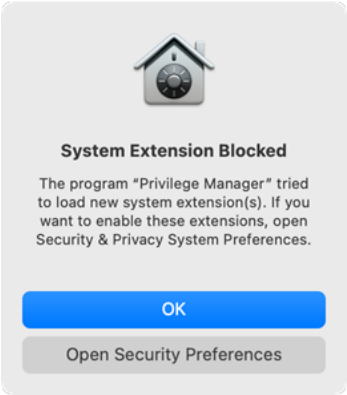
Notifications Approval

When presented with the Privilege Manager Notifications dialog, click **Options** | **Allow**. This will ensure that you are notified via Notification Center when an approval request is allowed or denied.



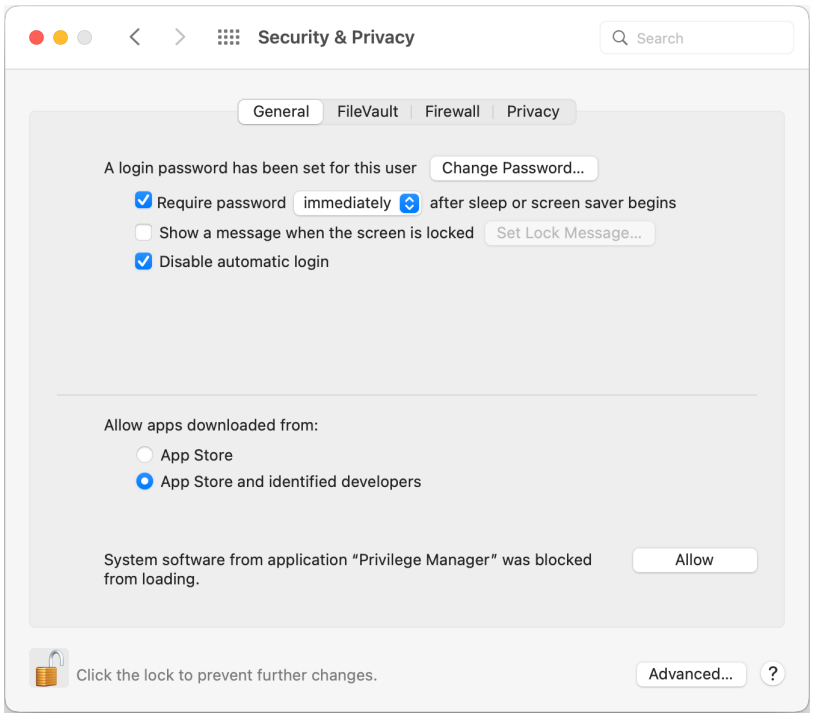
System Extension Blocked

When the installation completes, macOS will present the following dialog, prompting you to acknowledge that Privilege Manager tried to load a new system extension. Click **Open Security Preferences** to allow the system extension.

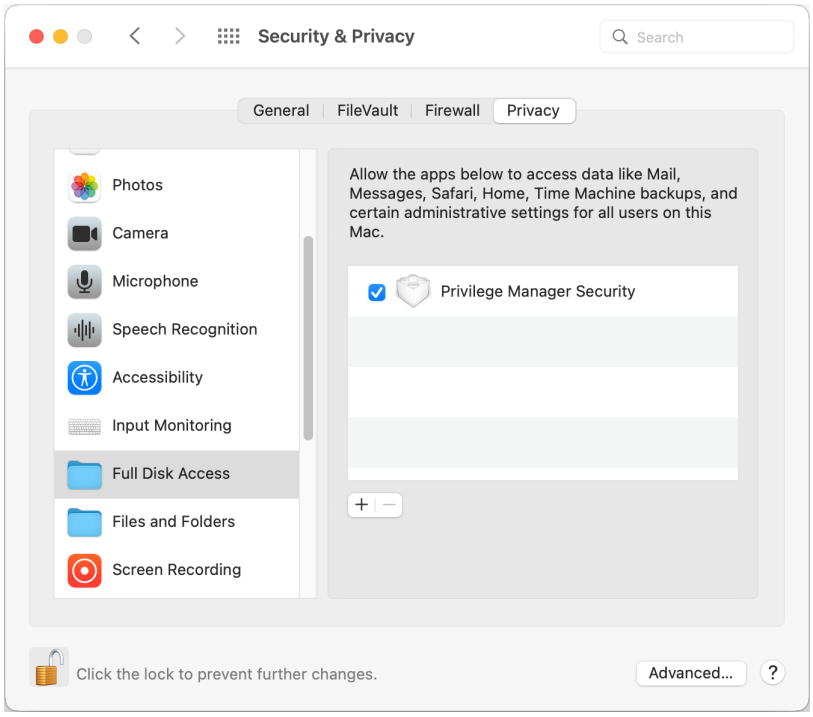


If you click **OK**, you will need to open **System Preferences** | **Security & Privacy** | **General** to allow the system extension.

To allow the system extension, click the padlock in the bottom left to enter Admin credentials and then click **Allow**.



Click the **Privacy** tab and use the scroll bar to select **Full Disk Access**, then select **Privilege Manager Security**.



The system extension is now properly configured to enforce policy.

Using an Unattended Install Method

After downloading the latest bundled macOS Agent package onto one of your macOS endpoints, extract the DelineaManagementAgent-n-n-nnnn.pkg installer from inside the DMG and upload it to your MDM's distribution point.

Create a policy to include the newly uploaded installer package, and include the script below to run before the package installation. Replace the values for `tmsBaseUrl` and `installCode` as required. `loginProcessingDelayS` has a default value of 30 (seconds). The `validateServerCertificate` setting controls whether the endpoint agent validates the Privilege Manager server's certificate when communicating with the server; set the value to 1 to enable validation. The default value is 0 for backward compatibility.

Refer to this video demonstration.

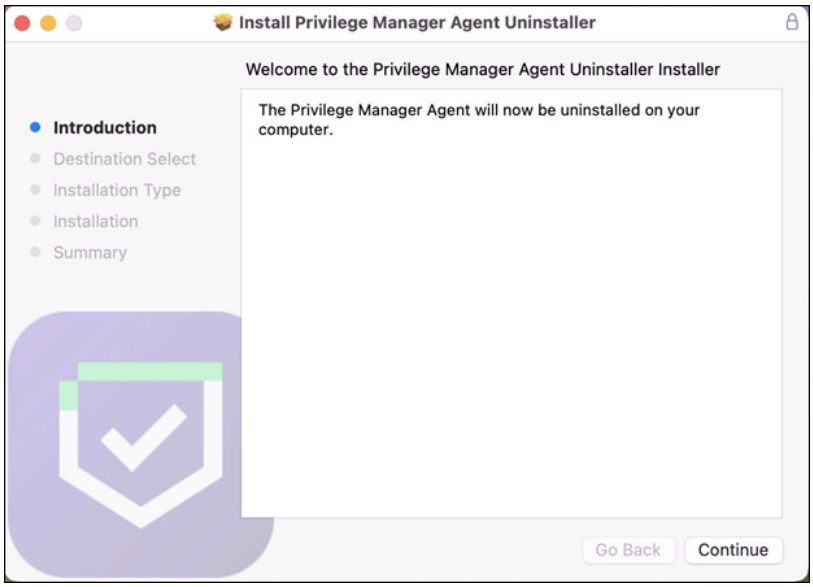
Note: Replace the version placeholders with the real package file version numbers.

```
#!/bin/zsh
# Verify Privilege Manager macOS configuration script to be used with a "vanilla" download
of the agent.
# This script should be used as a pre-install payload to run prior to the installation of
the PKG.
# Replace the tmsBaseUrl with your own server url i.e "https://your.privman.com/TMS"
# Replace installCode with your own details.

/bin/mkdir -p /Library/Application\ Support/Delinea/Agent/

/bin/cat << EOF > /Library/Application\ Support/Delinea/Agent/agentconfig.json
{
      "tmsBaseUrl": "",
      "installCode": "",
      "loginProcessingDelayS": 30,
      "validateServerCertificate": 0
}
EOF
sleep 5
```

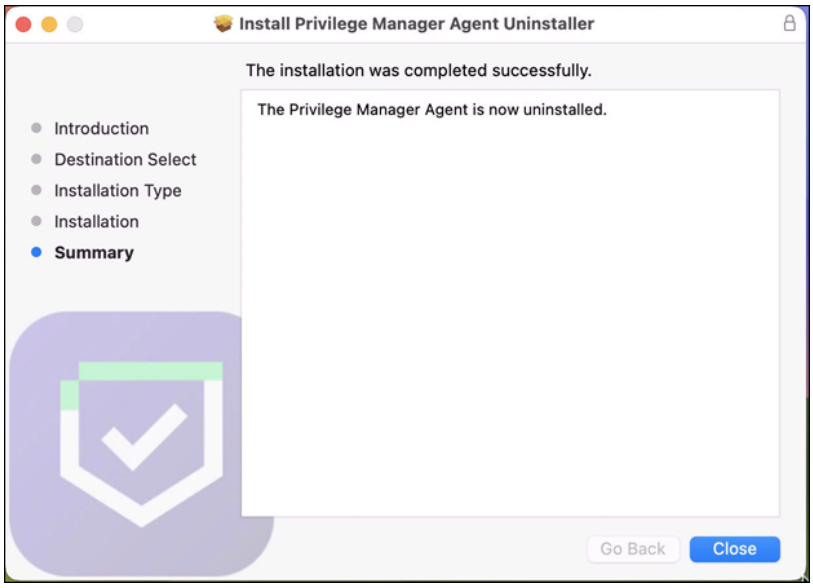
Note: It will take 15-30 minutes for newly installed agents to register in Privilege Manager. See the agent registration information in the Terminal Commands topic to speed the process up.

Uninstalling an Agent

In the 11.4.3 agent, instead of using a shell script to uninstall the agent, there is now an uninstaller .pkg file. When you need to uninstall the macOS agent, mount the .dmg file and use the Uninstaller.pkg package.



There will be prompts for admin credentials throughout the process. Once the uninstaller has finished, this screen is displayed.



Uninstall.sh

If the Uninstall.sh script is still needed to add to an existing script-based workflow, it can be run as follows:

```
sudo <pathToDownloadedUninstallScript>/Uninstall.sh
```

Verification

Running `pkgutil - -files com.delinea.agent` should report the following:

No receipt for 'com.delinea.agent' found at '/'.

Deploying Uninstaller.pkg with an MDM

Removing a system extension requires that the end user supply admin credentials, unless the system extension was installed silently using an MDM Configuration Profile with a System Extension whitelist payload. See "Using MDM Profiles for your Agent" on page 194.

If this is the case in your environment, it is possible to uninstall Privilege Manager without end user interaction via Jamf or MDM using these steps.

1. Remove the deployed system extension whitelist profile from the endpoint. This will terminate the system extension.

   Note: Unloading the system extension WILL DISABLE THE AGENT.

2. Push out the Uninstaller.pkg via policy to uninstall Privilege Manager.
3. An endpoint reboot is not required, but the terminated system extension will remain installed and inactive until reboot.

Installing Windows Agents

Important: When installing the agent for the first time or upgrading from a previous version, review the information presented in "Reboot Requirements - Windows Agents" on page 29 to understand what conditions in the runtime environment will result in a required reboot of the computer in order for the install/upgrade to be completed properly and the agent to function properly. Failing to understand the reboot requirements in relation to your environment may result in the application control service or other components of the agent failing to function properly.

Agent System Requirements

For agents in an environment with a moderate policy configuration, the requirements for memory and disk space are as follows:

- Memory usage: 50Mb
- Disk usage:
  - Delinea base agent: 10MB
  - Application Control Solution: 9MB
  - Local Security Solution: 3MB
  - Security Analysis Solution: 13 MB
- Average CPU over a week: 3%
- Impact to boot time: Negligible

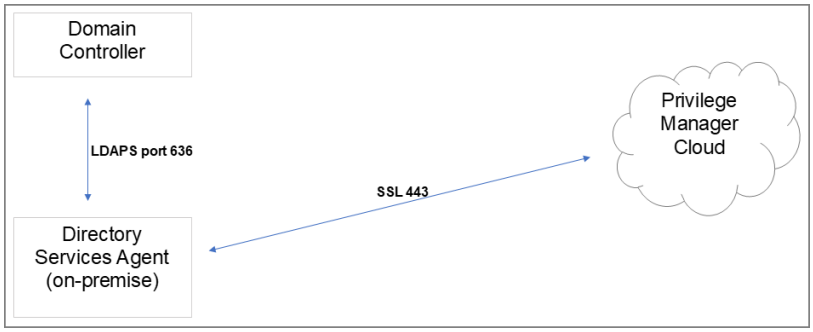
Directory Services Agent

The Directory Services Agent needs to be installed on a well resourced system running either

- Windows 10 or above
- Windows Server 2016 or above.

- Port requirements:
  - The agent needs to be able to communicate to the server on 443
  - AD Sync agent and Domain Controller over LDAPS

Note: The Directory Services Agent is available for x64-bit systems only.



Supported Windows Operating Systems (both 32- and 64-bit) on Systems Considered Workstations:

- Desktops: Windows 10, Windows 11
- Servers: Windows Server 2012 R2 and newer
- **Disable** the GPO security option "System cryptography: Use **FIPS** compliant algorithms for encryption, hashing, and signing."

Bundled Install

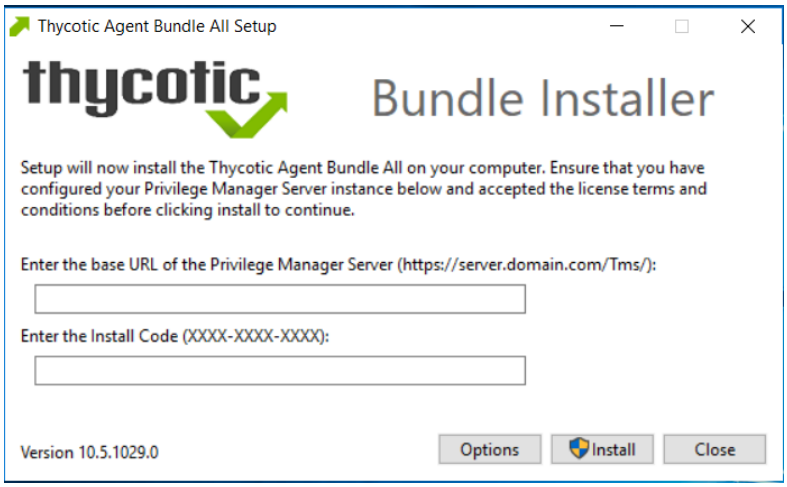
The bundled EXE installer includes all Privilege Manager Agents for Windows machines (Core, ACS, LSS), replacing the three separate deployments previously required. You can use the bundled installer directly on individual endpoints for testing or for production environments in either 32-bit or 64-bit environments.

Important: To ensure you have installed all prerequisite software on your managed computers **before** you install the Delinea agents, please see our System Requirements for Privilege Manager and Agent System Requirements.

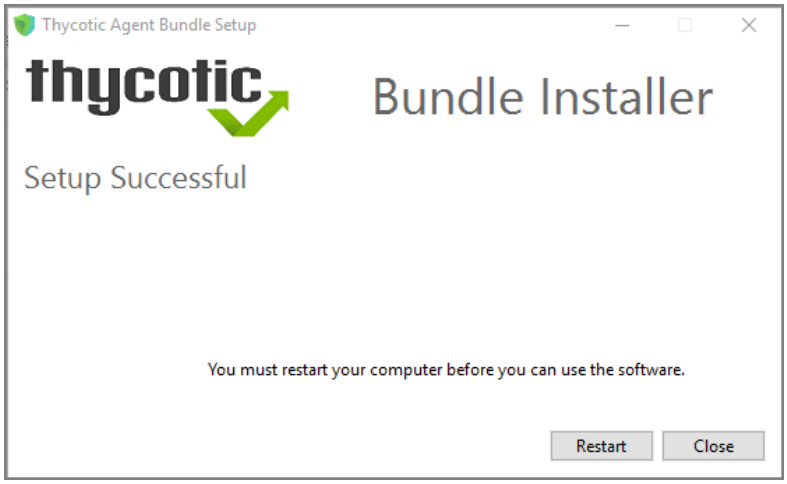
To install Delinea agents **on a single testing machine**, follow these steps:

1. Download the Bundled Agent Installer - Windows.
2. Run the Delinea Bundled Installer on the computer you want to manage.
3. During the setup process, enter the Privilege Manager Server URL (or AZ Service Bus Queue URL) and the Install Code when prompted.

   Note: The Install Code field can be left blank when using versions lower than 10.5.



4. After the installation you will be prompted to restart your endpoint.



Note: The bundled installer does require a restart in order to ensure the agent is completely ready to use.

Rollout to Multiple Systems

To install Delinea agents **on multiple machines**,use the following command line:

```
PMAgents_11_4_3215.exe /quiet /norestart ServerUrl=https://{servername}/Tms/
InstallCode=5Z0NRFZJLPVZ
```

where:

- `/quiet` makes the install run quietly
- `/norestart` will prevent the installer from restarting the machine (but a restart may still be required, so a restart should be scheduled for any upgrade)

- `ServerUrl` sets the server URL (replace {servername} with your actual server name)
- `InstallCode` sets the install code (replace with a valid install code from your Agent settings. Refer to "Agent Install Codes" on page 61)

Bundled Uninstall

To uninstall, use the following command line:

```
PMAgents_11_4_3215.exe /uninstall /quiet /norestart
```

Bundled Core and Directory Services Agents

The **Thycotic Directory Services Installer** bundle delivers the Delinea Agent (Core Agent) and the Delinea Directory Services Agent in one package for installation on x64-bit systems.

We recommend to refer to the following topics before you proceed with the bundled installation:

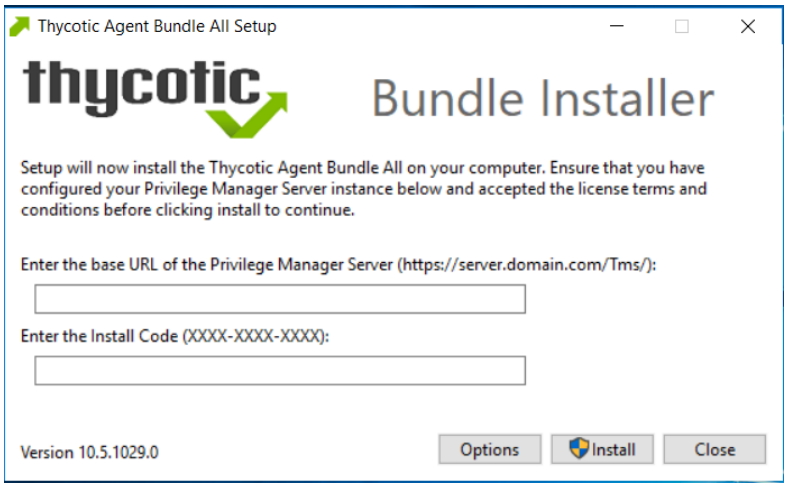
- Directory Services Agent (AD), to learn more about the **Directory Services Agent** itself.
- Active Directory Synchronization, to learn how to setup and run the synchronization task on the **Synchronization** tab of the **Active Directory Domain** foreign system.
- Agent System Requirements, to learn about the **Directory Services Agent** specific system requirements.

Installing the Delinea Directory Services Installer Bundle

To install this Delinea agents bundle **on a single machine**, follow these steps:

1. Download the Bundled Privilege Manager Core and Directory Services Agent - Windows.
2. Run the **ThycoticDirectoryServicesInstaller** on the computer you want to use for the active directory synchronization tasks.
3. During the setup process, enter the Privilege Manager Server URL (or AZ Service Bus Queue URL) and the Install Code when prompted.

   Note: The Install Code field can be left blank when using versions lower than 10.5.



4. Click **Close** after the installation completes.

> **Note:** It may take 15-30 minutes for agents to receive new policies, to speed this up navigate to **Admin | Configuration | General** and click **Run Policy Targeting Update**, then open the Agent Utility on the endpoint and click the **Register** button.

Directory Services Agent (AD)

This agent supports the Active Directory synchronization between Privilege Manager Cloud instances and local directory services. This agent only needs to be installed on one system to perform the synchronization task. The local agent can be deployed into an AD environment instead of requiring direct connectivity from the server to the domain controllers. You will be able to configure the product in either method (direct or agent-based).

The agent method requires that the Directory Services Agent is installed on one computer connected to a domain controller. Once installed, the agent receives the Active Directory Sync (Agent) scheduled task along with other parameters such as the credential used, which AD objects, etc. to perform a synchronization between a Cloud instance and local AD.

> **Note:** If the Directory Services Agent is installed on a system with an Application Control or a Local Security Agent, a license will be consumed. If a system has the Delinea Agent (Core Agent) and Directory Services Agent installed ONLY, no license is consumed.

The Directory Services Agent for local AD synchronization with Privilege Manager Cloud instances is available for x64-bit systems only.

If the Directory Services Agent produces error messages about failed application control policy processing in the agent log, those messages can be ignored.

When upgrading Privilege Manager to a newer version, it is recommended to also upgrade the Directory Services Agent so they are both on the same version.

We recommend the following topics for details pertaining to the **Directory Services Agent** functionality:

- Active Directory Synchronization, to learn how to setup and run the synchronization task on the **Synchronization** tab of the **Active Directory Domain** foreign system.
- Agent System Requirements, to learn about the **Directory Services Agent** specific system requirements.

Prerequisites

The **Core Delinea Agent** needs to be installed on the system that receives the **Directory Services Agent** installation. The other agents aren't required, but can be installed on the same system without issues.

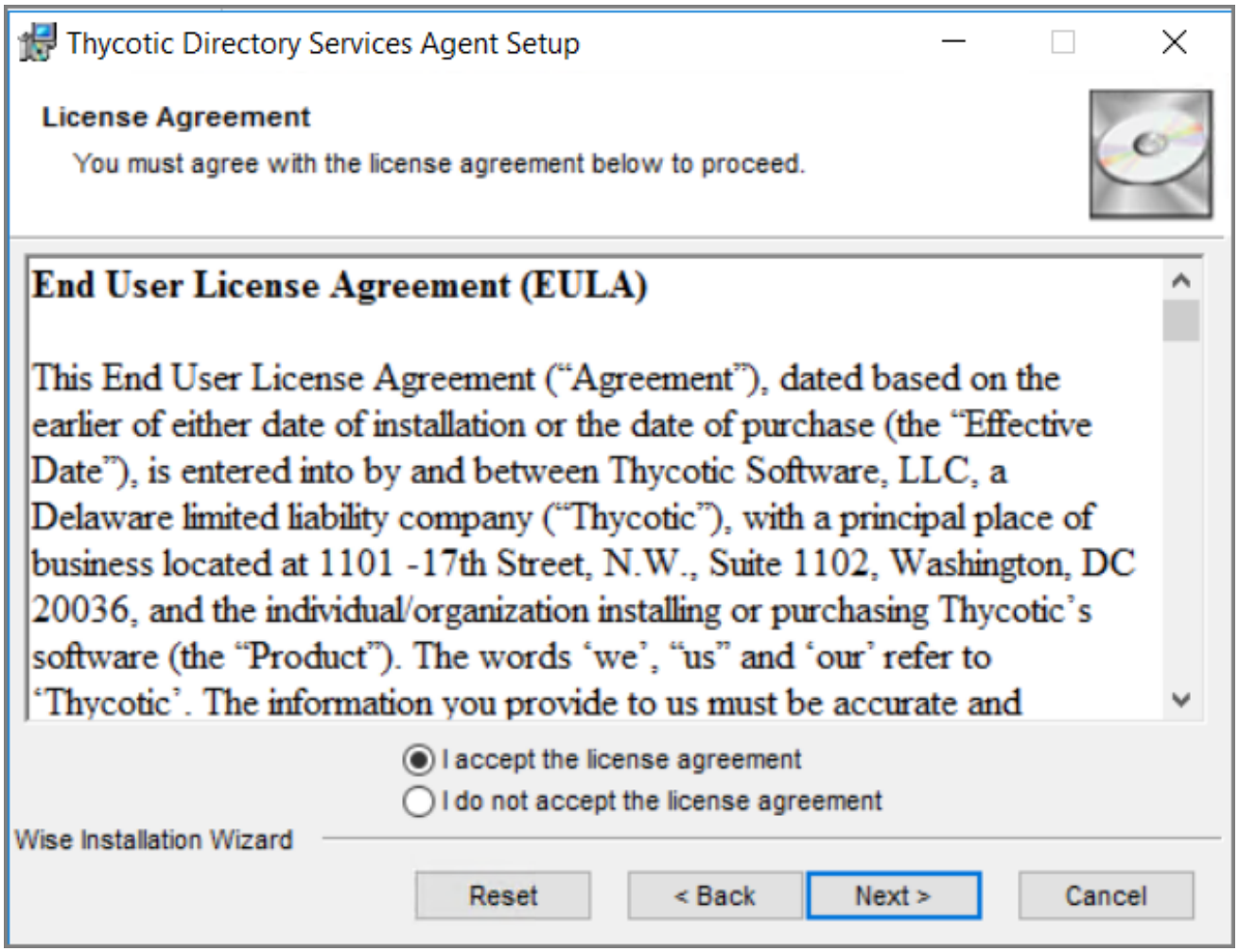
Directory Services Agent Installation

Download the latest version of the **Directory Services Agent** via the Software Downloads page.

1. Double-click the .msi file to start the installation wizard:

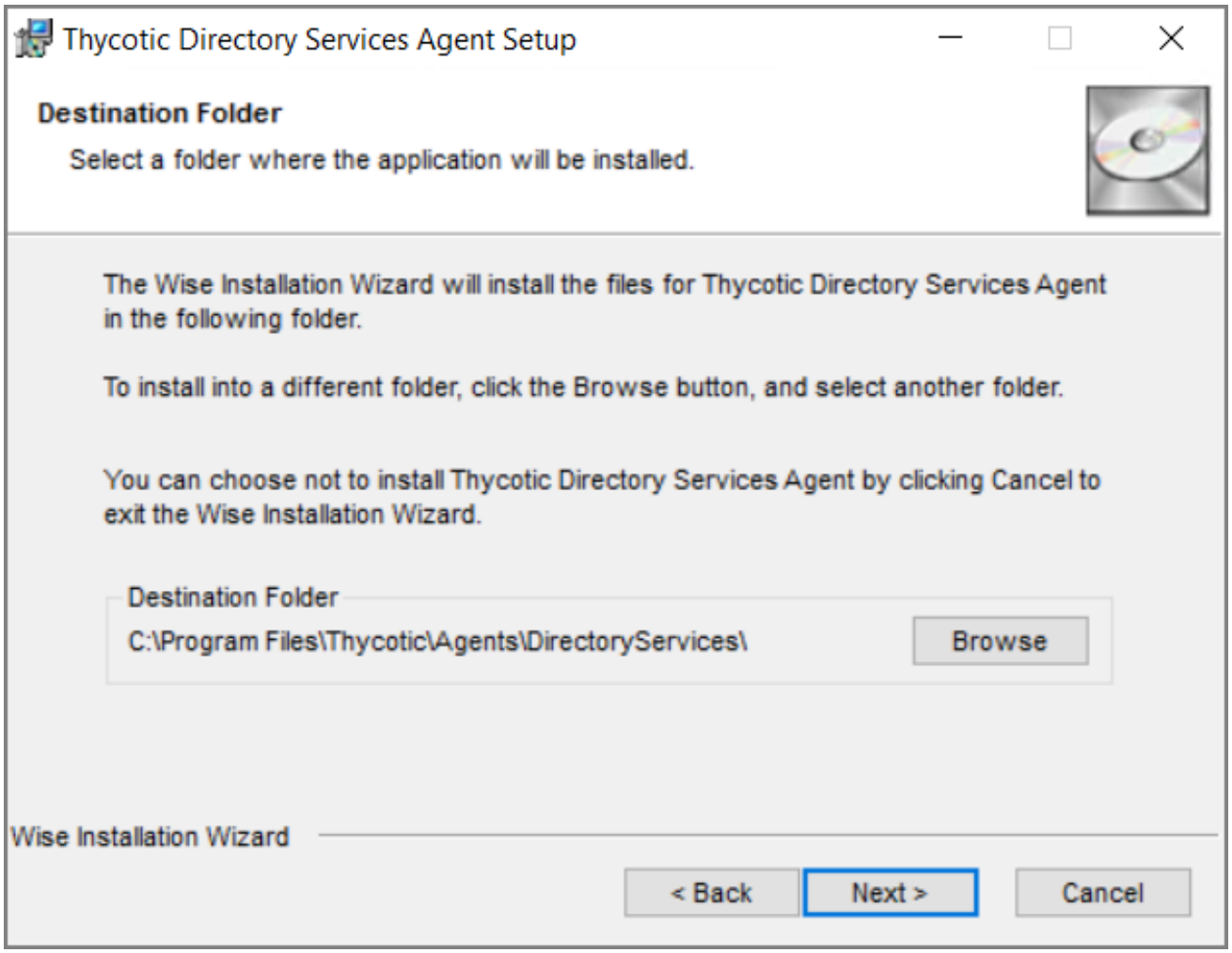
   Close all other applications running on the system and click **Next**.

2. On the **EULA Agreement** screen, select **I accept the license agreement**.



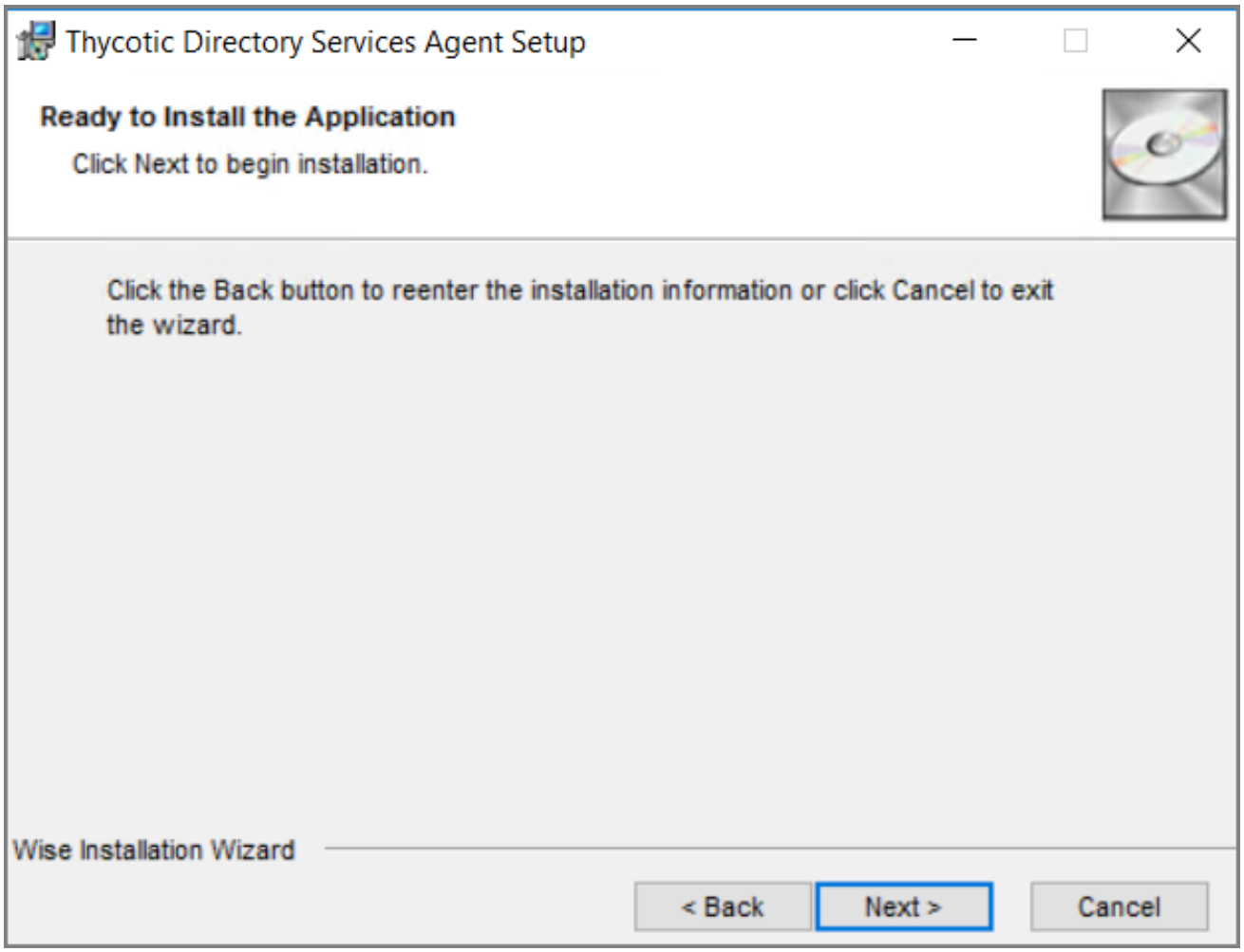
Click **Next**.

3. On the **Destination Folder** screen, keep the default installation destination or use **Browse** to select a different folder.



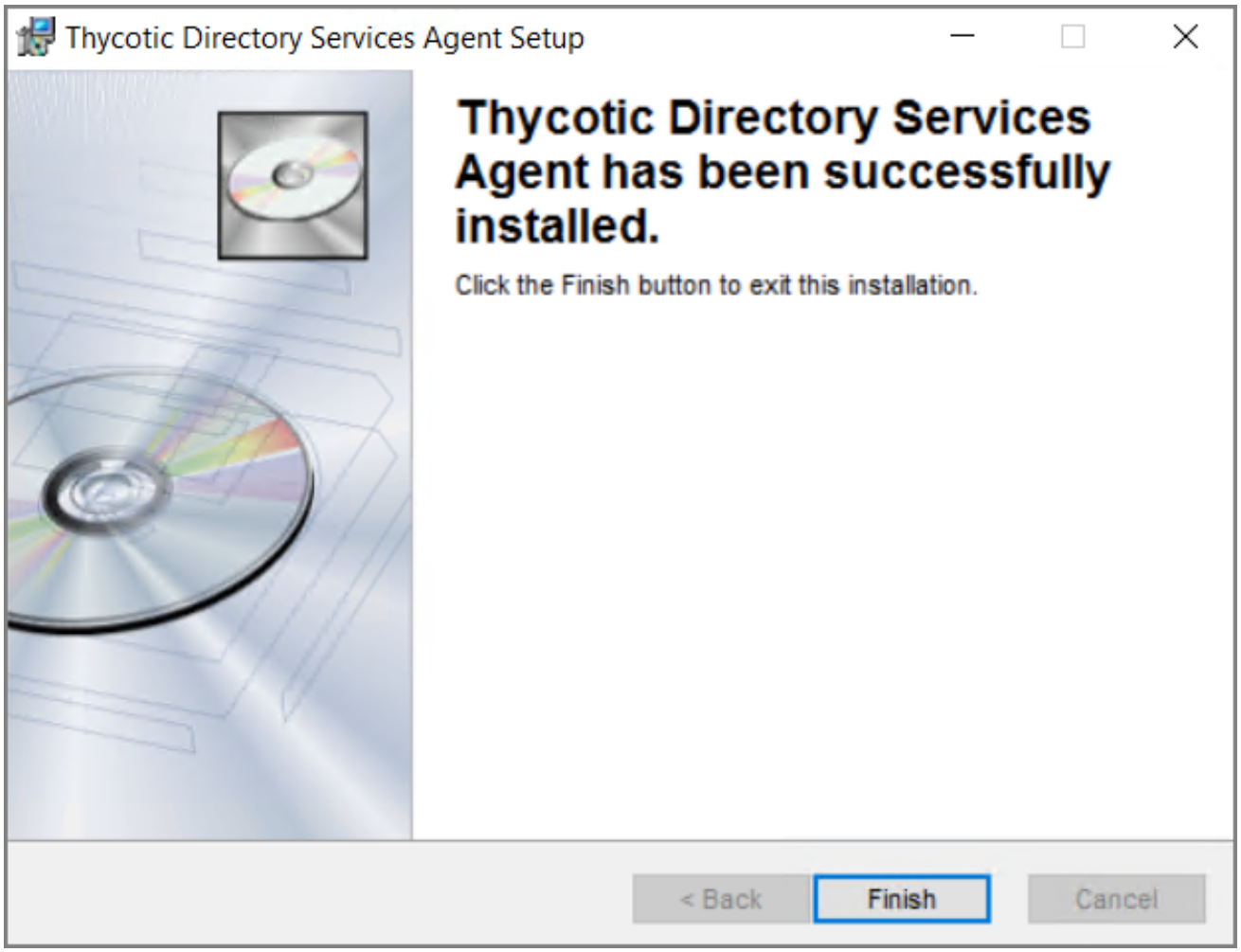
Click **Next**.

4. On the **Ready to install** screen, you have an option to go back to change your previous selection, otherwise click **Next** to proceed with the installation.



If you have any other Delinea Agents already installed on the system, the installer my prompt you to stop the services before you can proceed.

5. After a successful installation of the Directory Services Agent, you will see the following screen:



Click **Close**.

6. Restart any previously stopped agent services.

Windows Agents

Use the links below to download the agent installation software for Windows based endpoints.

There are three agents available for Windows endpoints:

- **Application Control Agent** (ACS): This agent is responsible for monitoring processes executing the Privilege ManagerApplication Control Functions on the endpoint.
- **Local Security Agent** (LSS): This agent is responsible for monitoring and executing Local Security functions.
- **Thycotic Agent**: The core agent is responsible for all reporting and monitoring communication on the endpoint. It can be considered the managing agent, while the Application Control and Local Security Agents are the worker agents.

Individual Agent Installers for Privilege Manager

Hardened Agents

If agent hardening was applied to user endpoints, the hardened agents need to be deleted via the `sc delete {agent name}` commandline command. This needs to be done under the context of the domain user prior to running the msi-based agent installation commands. When the agent is deleted successfully, a success message will be returned, for example:

```
C:\sc delete arelliaagent
[SC] DeleteService SUCCESS
C:\sc delete arelliaacsvc
[SC] DeleteService SUCCESS
```

Note: If the hardened agents are being deleted via software delivery script, the script needs to be delivered under the context of the domain user.

64-bit Windows Operating Systems

Individual Windows agents are available in MSI format for easier bulk-rollout through software delivery tools. For installing individual agents, ensure that the Core Delinea Agent is installed last.

Refer to the Software Downloads page for OS-specific downloads.

- Application Control Agent (x64)
- Local Security Solution Agent (x64)
- Core Thycotic Agent (x64)

Installation Command Lines

Note: The Install Code field can be left blank when using versions lower than 10.5

When installing agents, proper order of execution is crucial for proper registration of all components, as follows:

- Application Control Agent

```
msiexec.exe /i "Thycotic_ApplicationControlAgent_x64_11_3_7587.msi" /norestart
REBOOT=ReallySuppress /qn
```

- Local Security Agent

```
msiexec.exe /i "Thycotic_LocalSecurityAgent_x64_11_3_7585.msi" /norestart
REBOOT=ReallySuppress /qn
```

- Core Delinea Agent

```
msiexec.exe /i "ThycoticAgent_x64_11_3_7587.msi" /norestart
AMSURL=https://SERVERNAME/TMS/ INSTALLCODE=XXXX1234ABCD REBOOT=ReallySuppress /qn
```

32-bit Windows Operating Systems

Individual Windows agents are available in MSI format for easier bulk-rollout through software delivery tools.

When installing agents, proper order of execution is crucial for proper registration of all components, as follows:

- **Application Control Agent (x86)**
- **Local Security Solution Agent (x86)**
- **Core Thycotic Agent (x86)**

Refer to the Software Downloads page for OS-specific downloads.

Installation Command Lines

Note: The Install Code field can be left blank when using versions lower than 10.5

- Application Control Agent

```
msiexec.exe /i "Thycotic_ApplicationControlAgent_x86_11_3_7587.msi" /norestart
REBOOT=ReallySuppress /qn
```

- Local Security Agent

```
msiexec.exe /i "Thycotic_LocalSecurityAgent_x86_11_3_7585.msi" /norestart
REBOOT=ReallySuppress /qn
```

- Core Delinea Agent

```
msiexec.exe /i "ThycoticAgent_x86_11_3_7587.msi" /norestart
AMSURL=https://SERVERNAME/TMS/ INSTALLCODE=XXXX1234ABCD REBOOT=ReallySuppress /qn
```

Upgrades

Important: Before upgrading to version 11.4.2 or newer from version 11.4.1 & older, review the information presented in "Virtual Service Accounts" on page 90 completely and ensure that your runtime environment complies with the stated requirements. Failing to do so will result in the application control service failing to function properly.

Important: When installing the agent for the first time or upgrading from a previous version, review the information presented in "Reboot Requirements - Windows Agents" on page 29 to understand what conditions in the runtime environment will result in a required reboot of the computer in order for the install/upgrade to be completed properly and the agent to function properly. Failing to understand the reboot requirements in relation to your environment may result in the application control service or other components of the agent failing to function properly.

Troubleshooting Failing Upgrades

Upgrades may fail when spanning multiple versions. If an upgrade fails, the following workaround is available:

- The newer Privilege Manager versions use spSaveItemComplete, which won't be present if the database failed to upgrade. The work-around is to import a dummy version of spSaveItemComplete, which will be replaced by the correct version once the database is upgraded.

Note: If you are still running into upgrade issues, open a support ticket and schedule a support or professional services engagement session. Please plan accordingly, as support appointments may require advance scheduling up to five days.

Best Practices for Upgrades

DB Backup

Delinea recommends that Privilege Managerdatabases are backed-up prior to an upgrade. For details regarding SQL database backups, refer to the vendor documentation of your SQL database, such as Back Up and Restore of SQL Server Databases.

TMS Folder Backup

Other measures to take before any upgrade are to make a backup copy of your Privilege ManagerTMS folder and all its contents.

1. On your Privilege Managerhost system navigate to `C:\inetpub\wwwroot\TMS` (default installation location).
2. Create a backup copy of the TMS folder contents at another location on your system or network.

Repair Solution

When running into an error condition during an upgrade, try the repair option for the specific solution that errored out.

Also refer to Troubleshooting - Installation and Upgrade Issues.

Offline Upgrades

Follow these steps to perform an offline upgrade for Privilege Manager. This article is ONLY applicable when upgrading from versions 10.2 and higher.

Note: Offline upgrades on **multiple** servers will need to be done manually.

1. Download the latest version for the Privilege ManagerApplication Files via Software Downloads.
2. Extract the zip file.
3. From the unzipped folder, copy the contents of the nugetCache folder to this location on the web server: `C:\ProgramData\NugetCache\`
4. Navigate to the TMS web folder (`C:\inetpub\wwwroot\TMS\`), right-click and open with, e.g. **Notepad > Run as Administrator** the **web.config** file.
   a. Update the "value" field of this item `<add key="nuget:source:SolutionCentre" value="http://tmsnuget.thycotic.com/nuget/" />` to `C:\ProgramData\NugetCache\`, such as

      ```
      <add key="nuget:source:SolutionCentre" value="C:\ProgramData\NugetCache\" />
      ```

   b. Save the **web.config** file.
   c. Recycle the TMS app pools.
5. Navigate to `https://<webserver>/TMS/Setup/ProductOptions/ShowProducts`. This step will require windows authentication using an account that has local administrator permissions on the web server.
6. You should see new products available in the products list. Click the **Install/Upgrade Products** button.
7. Select the products you wish to upgrade or install, and follow the steps to finish the installation. If one of the products fails to install, please repeat these last two steps. You may encounter an issue with an error of "Version Store out of Memory" - this is transient and re-starting the upgrade will fix it. If you encounter any additional errors, please contact Delinea Technical Support for assistance.

> **Note:** An upgrade or repair to the product may rewrite the web.config with default settings. Always double-check that the web.config has the correct SolutionCentre path whenever you perform a manual upgrade. Also, the version numbers available should match the highest versions available in the C:\ProgramData\NugetCache\ folder on the web server.

Delinea recommends to create a back-up copy of the Privilege Managerweb application folder after installation or upgrades.

Offline Upgrades - Combined

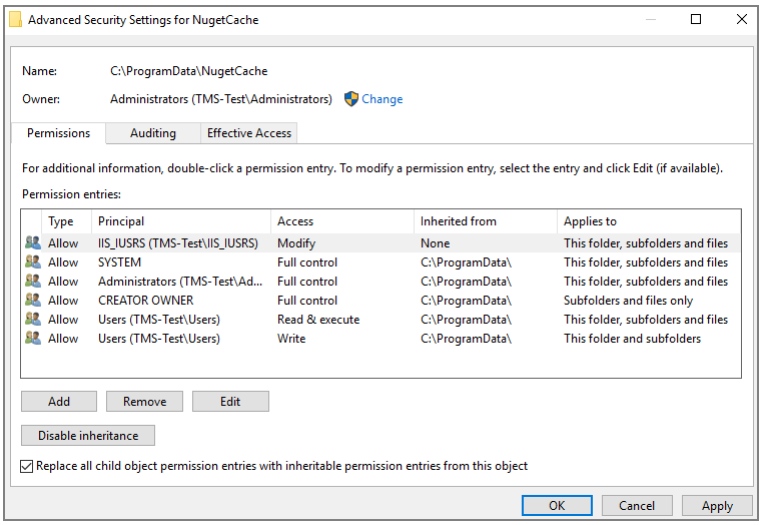
Follow these steps to perform an offline upgrade for Privilege Managerand Secret Server. This topic is ONLY applicable when upgrading from products that are versions 10.2 and higher.

> **Note:** Offline upgrades on **multiple** servers will need to be done manually. Also refer to the High Availability Setup topic for general best practices.

1. Download the zip files for your offline upgrade here. Copy/paste this zip file on your Privilege ManagerWeb server
2. Make a backup of the Secret Server and Privilege Managerweb folders (Default path is `C:\inetpub\wwwroot>SecretServer + TMS` folders, copy/paste these into a backup folder)
3. Make a backup of the Database (In Secret Server navigate to Admin | Backup | Backup Now button)

4. On the web server, navigate to `C:\ProgramData\NugetCache\` and delete all the files in the folder (*ProgramData folder may be hidden: View > check the Hidden items box to reveal)
5. Open Secret Server and navigate to: `https://<YourSecretServerURL>/Setup/Upgrade`
6. On the Secret Server Update page:
   a. Select **Advanced (not required)** to open the advanced options.
   b. Select **Choose File** and navigate to the location of the Privilege ManagerUpdate zip package.
   c. Select **Upload Upgrade File**.
   d. When the new version is available select **Upgrade**.

      Check `https://URL/TMS/Setup` to see if an install is already in progress (this is usually seen when the TMS Upgrade portion of SS shows successful)
7. Accept the License. Then allow the Secret Server upgrade to complete. Note that the Upgrade TMS step may say it was successful, or it may say it wasn't. Please ignore this message and continue to follow the steps below:
8. Open the `C:\ProgramData\` folder:
   a. Right-click on the NugetCache folder and select **Properties**.
   b. Click on the **Security** tab.
   c. Click the **Advanced** button.
   d. Check the **Replace all child object permission entries with inheritable permission entries from this object** checkbox



   e. Click the **OK** and **Yes**.
9. Navigate to the TMS web folder (`C:\inetpub\wwwroot\TMS\`), right-click and open with, for example, **Notepad > Run as Administrator** the **web.config** file.
   a. Update the "value" field of this item `<add key="nuget:source:SolutionCentre" value="http://tmsnuget.thycotic.com/nuget/" />` to `C:\ProgramData\NugetCache\`, such as

```
<add key="nuget:source:SolutionCentre" value="C:\ProgramData\NugetCache\" />
```

b. Save the **web.config** file.

c. Recycle the TMS app pools.

10. Navigate to `https://<webserver>/TMS/Setup/ProductOptions/ShowProducts` The TMS setup page requires authentication with a Windows account that is a Local Administrator of the Web Server.
11. You should see new products available in the products list. Click the **Install/Upgrade Products** button.
12. Select the products you wish to upgrade or install, and follow the steps to finish the installation. If one of the products fails to install, please repeat these last two steps. You may encounter an issue with an error of "Version Store out of Memory" - this is transient and re-starting the upgrade will fix it. If you encounter any additional errors, please contact Delinea Technical Support for assistance.

> **Note:** An upgrade or repair to the product may rewrite the web.config with default settings. Always double-check that the web.config has the correct SolutionCentre path whenever you perform a manual upgrade. Also, the version numbers available should match the highest versions available in the C:\ProgramData\NugetCache\ folder on the web server.

Delinea recommends to create a back-up copy of the Privilege Managerweb application folder after installation or upgrades.

Online Upgrades

Privilege Managersoftware updates are made available via NuGet server packages. The upgrade process can be performed via **Add/Upgrade Features** link in the Privilege ManagerSetup page.

What's New in Privilege Manager10.8

The 10.8 release of Privilege Managerintroduces a new user interface, providing a redesigned user experience, simplifying many major areas and typical workflow processes when setting up application policies or local security.

To preview the enhancements made to the user interface, please view this video.

Switching between the new and old UI post upgrade is not available.

Setting up the NuGet Source

Once Privilege Manageris installed on a server, updates can be performed by pointing the web.config file to the product NuGet source.

1. Navigate to `C:\inetpub\wwwroot\TMS\` and right-click the web.config file.
2. Select Edit from the drop-down.
3. Verify the following line with correct NuGet source is present:

```
<add key="nuget:source:SolutionCentre" value="http://tmsnuget.thycotic.com/nuget/" />`
```

Updating Privilege Manager

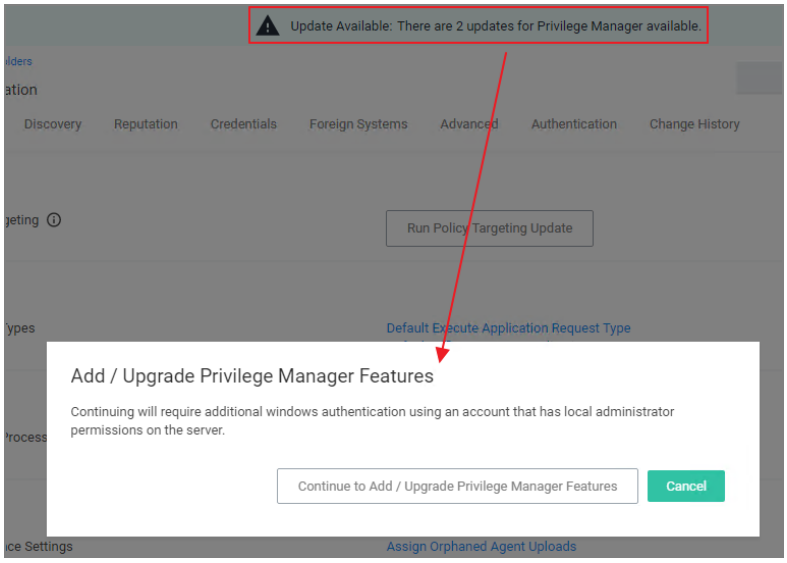
Note: Always make a backup of the Privilege ManagerDatabase in SQL and the TMS web files before performing upgrades in a production environment. The default location of the web files on the Privilege ManagerServer is `C:\inetpub\wwwroot\TMS`.

On systems running Privilege Manager10.5.1 or older with multiple Privilege ManagerServer nodes, **stop** the TMS application pools on all secondary nodes before starting the upgrade. Restart the applications pools once the upgrade is completed. Newer Privilege Managerversions automatically initiate setup tasks when the primary node is being updated.

Primary Node

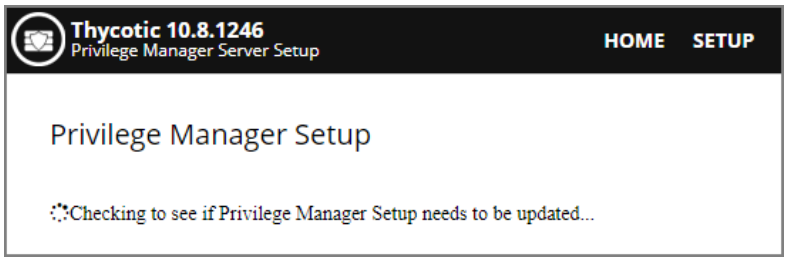
Privilege Managerprovides an **Update Available** notification banner when updates are available. Users can also use the **Admin | Setup** menu to enter the check if an update is available.

1. Click the link in the banner to trigger the **Add / Upgrade Privilege ManagerFeatures** modal:

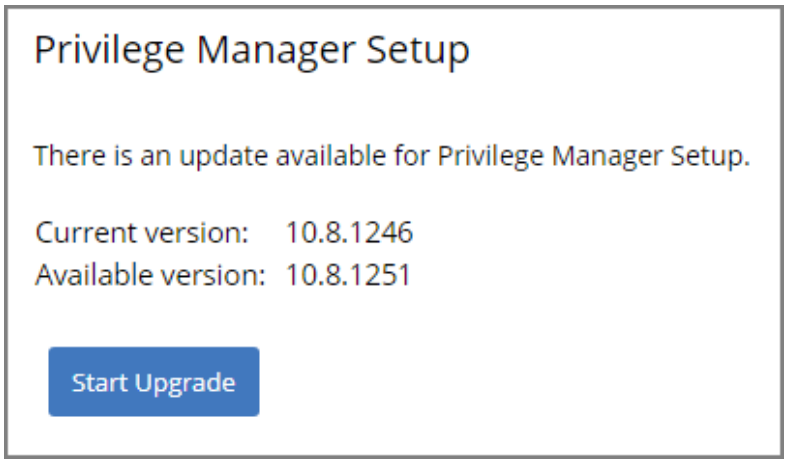


If you are not a local Administrator on the server, you will not be able to perform the upgrade. Based on your account role membership either click **Continue to Add / Upgrade Privilege ManagerFeatures** or **Cancel** if your role permissions don't meet the requirement.

This starts the process to see if setup updates are available.

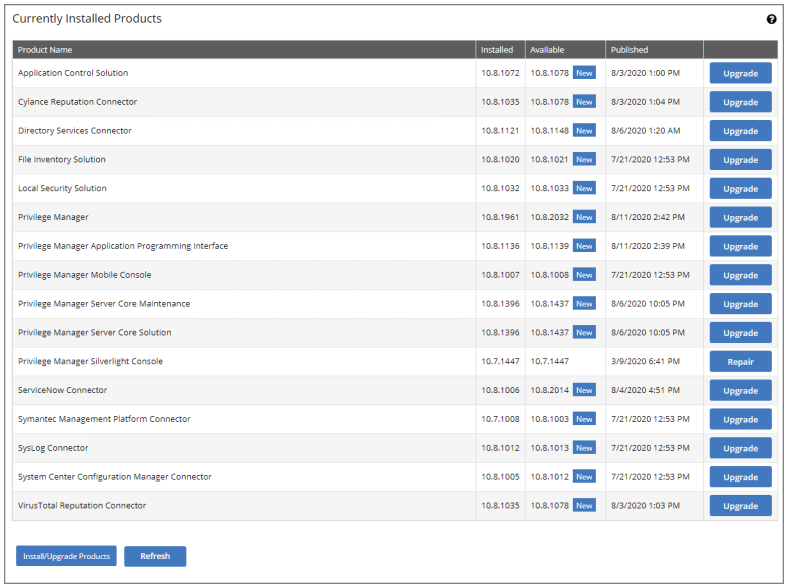


2. When updates are available, Privilege Managerwill provide information about the current and available versions.



Click **Start Upgrade**.

3. A short *Install Complete* message is displayed before the setup process navigates to the **Currently Installed Products** page. The available product updates are listed by product name in alphabetical order.



Currently Installed Products

Product Name	Installed	Available	Published	
Application Control Solution	10.8.1072	10.8.1078 New	8/3/2020 1:00 PM	Upgrade
Cylance Reputation Connector	10.8.1035	10.8.1078 New	8/3/2020 1:04 PM	Upgrade
Directory Services Connector	10.8.1121	10.8.1148 New	8/6/2020 1:20 AM	Upgrade
File Inventory Solution	10.8.1020	10.8.1021 New	7/21/2020 12:53 PM	Upgrade
Local Security Solution	10.8.1032	10.8.1033 New	7/21/2020 12:53 PM	Upgrade
Privilege Manager	10.8.1961	10.8.2032 New	8/11/2020 2:42 PM	Upgrade
Privilege Manager Application Programming Interface	10.8.1136	10.8.1139 New	8/11/2020 2:39 PM	Upgrade
Privilege Manager Mobile Console	10.8.1007	10.8.1008 New	7/21/2020 12:53 PM	Upgrade
Privilege Manager Server Core Maintenance	10.8.1396	10.8.1437 New	8/6/2020 10:05 PM	Upgrade
Privilege Manager Server Core Solution	10.8.1396	10.8.1437 New	8/6/2020 10:05 PM	Upgrade
Privilege Manager Silverlight Console	10.7.1447	10.7.1447	3/9/2020 6:41 PM	Repair
ServiceNow Connector	10.8.1006	10.8.2014 New	8/4/2020 4:51 PM	Upgrade
Symantec Management Platform Connector	10.7.1008	10.8.1003 New	7/21/2020 12:53 PM	Upgrade
SysLog Connector	10.8.1012	10.8.1013 New	7/21/2020 12:53 PM	Upgrade
System Center Configuration Manager Connector	10.8.1005	10.8.1012 New	7/21/2020 12:53 PM	Upgrade
VirusTotal Reputation Connector	10.8.1035	10.8.1078 New	8/3/2020 1:03 PM	Upgrade

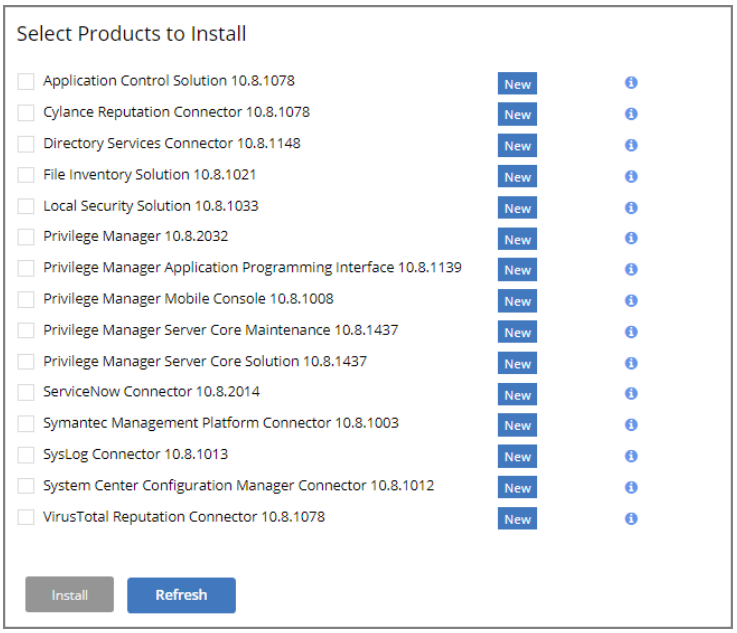
Install/Upgrade Products Refresh

Use either of the following ways to upgrade your environment to the latest Privilege Managerversion:

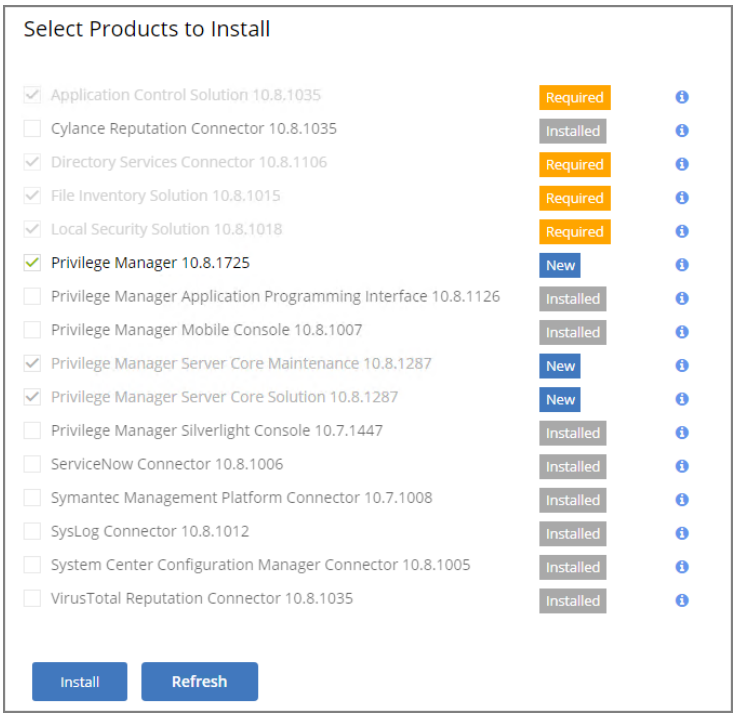
a. Click Upgrade next to individual packages, this will require to come back to the Installed Products page after each separate upgrade for most of the packages, **or**

b. Click **Install/Upgrade Products** at the bottom of the page.

   i. Select the products you want to install/upgrade.



   By default the products available for upgrade are listed. If you want to see all products currently installed, click **Show installed products**.



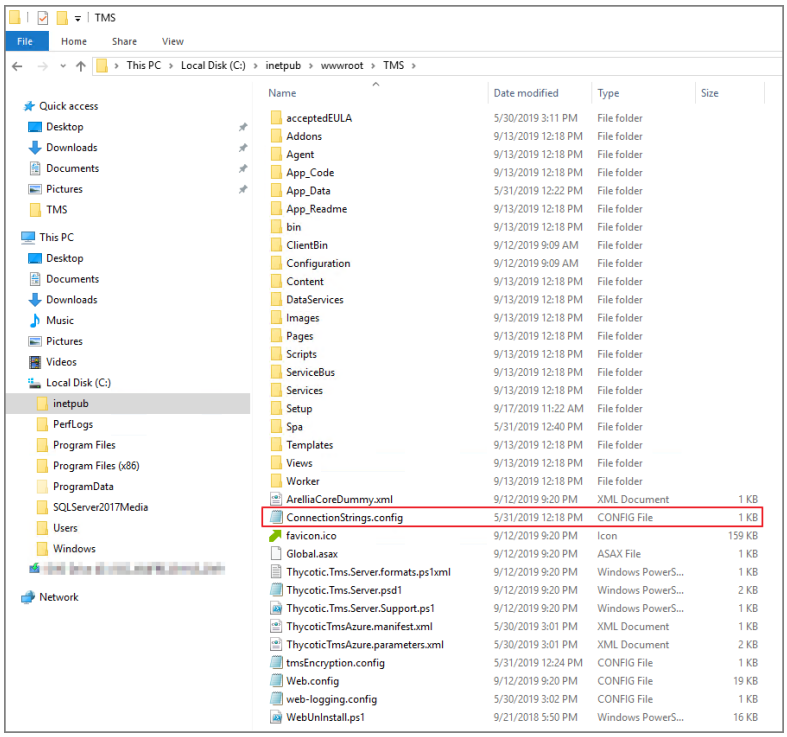
ii. Click **Install**.

The installation/upgrade process starts and you can view the log while products are being installed.

Secondary Nodes

Note: This is only required on Privilege Managerservers being upgraded from versions prior to **10.5.1**.

1. On the upgraded primary node navigate to TMS web files. The default location is: `C:\inetpub\wwwroot\TMS`.
2. Copy the TMS folder, except for the ConnectionStrings.config file.



3. On your secondary node navigate to the same folder location, most likely `C:\inetpub\wwwroot\TMS` and paste the copied files.
4. Repeat the copy and paste for all other secondary Privilege Managernodes in your environment.
5. Navigate to the IIS Manager and start all TMS Application pools on the secondary nodes.

Upgrading from Arellia Management Server 8.2 to Privilege Manager 10.4 and up

Upgrading from our 8.2 version to Privilege Manager 10.4 and up can't be done from `https://servername/Ams/Setup/`. To upgrade, we recommend using the same database and removing the old application before installing the new version. This can be done automatically or manually.

Automatic Steps

1. Download http://tmsnuget.thycotic.com/Software/ThycoticTmsInstaller_10_0_1570.exe and run it on the web server where your existing Arellia Management Server 8.x version is installed.
2. Follow the prompts.
3. Once it completes, you'll access the server at `https://servername/Tms/` instead of `https://servername/Ams/`.
4. Go to `https://servername/Tms/Setup` to install the latest 10.x version.
5. Open **IIS Manager** and go to **Sites** | **Ams** | **Agent** | **Uploads**.
6. Click on the **BITS Uploads** and change the notification URL from `http://localhost/Ams/Services/BitsUpload.ashx` to `http://localhost/Tms/Services/BitsUpload.ashx`.

7. Download and install and the latest agents. Please refer to the agent installation section the lastest agent installation.

   Note: Old agents will continue to work because of the redirect created during the install that sends traffic from `https://servername/Ams/Agent` to `https://servername/Tms/Agent`. When upgrading the agents, we recommend that you set the **AMSURL** to the new `https://servername/Tms/` address.

Manual Steps

1. Remove the AMS website from the web server.
2. Download the latest bundled installer http://thycotic.com/products/secret-server/resources/download-secret-server/.
3. Follow the prompts to install Privilege Manager, setting the database connection to the existing database.
4. Download and deploy the latest agents that are available here.

   Note: Set the AMSURL to the new server address, https://servername/Tms/

Virtual Service Accounts

Version 11.4.3 (build 11.4.3235) and Version 12.0.0 (build 12.0.1016)

Usage of virtual service accounts was completely removed from the application control service. As part of that change, ArelliaACSvc.exe is now running as **NT AUTHORITY\SYSTEM** instead of as a virtual service account.

Version 11.4.2

Starting with version 11.4.2, the Thycotic Application Control service (ACS), running the program ArelliaACSvc.exe, is configured to run using a virtual service account named **NT SERVICE\ArelliaACSvc** instead of the built-in **NT AUTHORITY\SYSTEM** (LocalSystem) account.

Important: Before upgrading to version 11.4.2 or newer from version 11.4.1 & older, review this information completely and ensure that your runtime environment complies with the stated requirements. Failing to do so will result in the application control service failing to function properly.

Note that virtual service accounts really are "virtual," in that there isn't a user account being provisioned on the computer, and there is no associated password that needs to be managed. Virtual accounts were first introduced in Windows 7 SP1, and they exist to allow specific sets of privileges and rights to be granted to specific native NT services in a fine-grained tightly-controlled manner.

Starting with Windows 8.1, it became possible to run the **LSASS.EXE** system process as PPL (Protected Process Light). This process is responsible for authenticating credentials, creating logon sessions and storing password hashes that are used to perform remote authentication when accessing file shares on remote servers. Microsoft introduced this capability to reduce the attack surface of Windows by preventing credential-theft attacks from succeeding when performed against the **LSASS.EXE** system process.

Initially, this capability was optional and disabled by default, although it could be enabled via the registry. Later, Microsoft increased the security of the **LSASS.EXE** system process again by allowing the enablement of **LSASS.EXE** running as PPL to be controlled via an UEFI variable and for the setting to be protected by the Secure Boot mechanism.

With Windows 11 22H2, **LSASS.EXE** running as PPL is enabled by default on all new installations (e.g., not upgraded from a prior build of Windows 11 or an older version of Windows). It is expected that Microsoft will continue to increase the security of the **LSASS.EXE** system process in future builds of Windows 11 as well as in whatever new version of Windows ends up being delivered as a successor to Windows 11.

Prior to version 11.4.2, all versions of the agent were entirely dependent on being able to obtain a copy of the process access token of the **LSASS.EXE** system process for the Thycotic Application Control service to be able to run properly. When the **LSASS.EXE** system process runs as PPL, it is no longer possible for the process token to be accessed by any other process running on the system, including services running as **NT AUTHORITY\SYSTEM**. The reason for the token copying to be performed had to do with the level of privilege required to perform token elevation operations. The Windows SCM (Service Control Manager), running in the **SERVICES.EXE** system process, has less privileges than the **LSASS.EXE** system process. It is not possible for the SCM to create a native NT service process running as **NT AUTHORITY\SYSTEM** that runs with more privileges than itself, even though the SCM itself runs as **NT AUTHORITY\SYSTEM**, too. The SCM can also start a service running under either the **NT AUTHORITY\NETWORK SERVICE** or **NT AUTHORITY\LOCAL SERVICE** accounts, too, but both of those accounts have less privileges than the SCM's own process which runs as **NT AUTHORITY\SYSTEM**.

The intersection of those limitations of the SCM and native NT services running as **NT AUTHORITY\SYSTEM** and the **LSASS.EXE** system process running as PPL made it necessary to make a change in how the Thycotic Application Control service (ACS) is configured, along with corresponding code changes, and is the reason for usage of a virtual service account to be adopted. When the SCM starts a native NT service process running as a virtual service account, the LSA privileges assigned directly to the virtual service account as well as any privileges assigned to local groups in which it has membership are all included in the service process's access token. This permits a native NT service to be started such that it runs with greater privileges than the SCM runs with. When the virtual service account **NT SERVICE\ArelliaACSvc** is properly configured with the LSA privileges and logon rights that are required, it can start up and run properly with the capability of performing token elevation operations.

Under no circumstances should manual modifications be made to the Thycotic Application Control service's configuration. The service is created and configured by the agent installer. After installation, any manual modification of the service configuration has the potential to break the service and necessitate an uninstall and reinstall of the agent to repair the service. The Thycotic Application Control service (ACS) is now configured to fail to start if the virtual service account **NT SERVICE\ArelliaACSvc** is lacking any of the required LSA privileges and/or logon rights.

> **Note:** Other agent-related services, such as the core agent service Thycotic Agent, are still configured to run as **NT AUTHORITY\SYSTEM**, as are all agent-related scheduled tasks running under the Windows Task Scheduler; all of them are completely unaffected by the virtual service account configuration requirements.

The following LSA privileges are granted to the virtual service account **NT SERVICE\ArelliaACSvc** by the installer:

- Act as part of the operating system
- Adjust memory quotas for a process
- Backup files and directories
- Bypass traverse checking
- Create a token object

- Create global objects
- Create permanent shared objects
- Create symbolic links
- Debug programs
- Impersonate a client after authentication
- Increase a process working set
- Increase scheduling priority
- Load and unload device drivers
- Manage auditing and security log
- Obtain an impersonation token for another user in the same session
- Perform volume maintenance tasks
- Profile single process
- Profile system performance
- Restore files and directories
- Take ownership of files or other objects

Every one of these LSA privileges are required and are essential to the proper operation of the Thycotic Application Control service (ArelliaACSvc.exe) now and in the future. If any of them are not granted to the virtual service account, the service will not start.

Additionally, the LSA logon right **Log on as a service** is required. On a new installation of Windows, the built-in group **NT SERVICE\ALL SERVICES** is granted **Log on as a service**, and all virtual service accounts automatically have membership in that group. This permits services configured to use a virtual service account to log on in service mode as the service is started. However, there are various security lock down or “hardening” recommendations that are frequently implemented which require that the **Log on as a service** logon right be revoked from **NT SERVICE\ALL SERVICES** and results in each virtual service account having to be explicitly granted the **Log on as a service** logon right.

It is very common for GPOs (Group Policy Objects) to be utilized in an enterprise Active Directory environment to push out security settings to endpoint computers where the agent gets installed. If one or more GPOs result in required LSA privileges and/or logon rights being revoked from the Thycotic Application Control service (ACS), then the service will fail to start. It will be necessary to modify one or more GPOs to make them comply with the virtual service account configuration requirements. One of the most common issues which occurs with trying to configure a GPO to meet these requirements is the inability to validate the virtual service account name **NT SERVICE\ArelliaACSvc**. If the agent is not currently installed on the computer where **GPEDIT.MSC** is being used to modify the GPO, then the service does not exist in the SCM’s configuration, and the virtual service account name cannot be resolved to a SID and thus is not able to be validated. One simple workaround for this issue is to create a dummy service named **ArelliaACSvc** on the computer where **GPEDIT.MSC** is being used, then modify the GPO, save the GPO, and finally, delete the dummy service.

The following commands can be used from an elevated **CMD.EXE** console window:

```
sc create ArelliaACSvc type= own start= demand binPath= C:\Windows\System32\nosuch.exe
sc sidtype ArelliaACSvc unrestricted
```

```
<In the GPO, add the "NT SERVICE\ArelliaACSvc" to the LSA privilege & logon right policy
settings as described above>
sc delete ArelliaACSvc
```

Getting Started

The steps for Getting Started vary, depending on whether you are implementing a cloud or on-premise instance of Privilege Manager.

Depending on your installation refer to either:

- "Getting Started Overview - Cloud" on page 98
- Getting Started - On-Premise

Deployment Types - Cloud vs. On-Premise

The following features and options are different from On-premises or previous Privilege Manager Cloud (10.7.x) releases:

- The ServiceNow connector is automatically installed for all new cloud instances.
- The SMTP server is automatically configured during the cloud instance setup.
- The setup is managed by Delinea and installations, upgrades, and repairs are unavailable to the customer directly, this includes setup, add/remove feature options, and connection options to existing Secret Server. Upgrade notices and banners are removed with upgrades being handled by Delinea during maintenance periods.
- All license key management is done via Delinea and license keys are not visible on the licensing page. There are presently no options for customers to add additional licenses directly.

The following features and options are **not** available in Privilege Manager Cloud:

- Server-side Powershell scripts not signed by Delinea are not allowed. Custom server-side work can be done via Professional Services engagements.

All other features and functionality of Privilege Manager On-premises and Cloud are the same unless otherwise specified.

Getting Started Overview - On-Premise

The following topics provide a guided path through the on-premise (on-prem) installation and setup steps that are part of the initial stand-up of an on-premises Privilege Manager deployment. For cloud specific getting started instructions refer to "Getting Started Overview - Cloud" on page 98.

Preliminary Configuration

Refer to these topics to learn more about the initial installation and setup steps.

1. System Requirements
2. Antivirus Exclusions
3. Privilege Manager Installation
4. Agents Installation
   - Setting the Server Address for Privilege Manager Agents, if the address provided during the agent installation requires updates.
5. Login
6. Licenses

Note: If you are targeting macOS based endpoints, refer to "Getting Started with macOS" on page 146.

Rollout Recommendation

Familiarize yourself with the Least Privilege concept. Delinea recommends a phased roll-out between the Application Control and Local Security, for example:

1. Application Control: Set up learning mode policies on a group of test endpoints to learn about applications running on your endpoint machines (Event Discovery | Learning Mode Policies - Send Policy Feedback)
2. Local Security: Begin managing your local user accounts (only) and defining local group membership (Local Security | Manage Local Users)
3. Application Control: Tailor your policies so that they won't disrupt employee work (Creating Policies | Elevation Policies) but will block known malicious applications (Creating Policies | Example: Quarantine Specified Malware). Implement these basic policies across agents in production
4. Application Control: Continue to tailor policies according to employee roles. Create a "Request Access" system for any unknown applications. (Creating Policies | Example: Application Execution Requires Approval (Workflow))
5. Local Security: Once a workflow has been established between employees and the Privilege Manager Helpdesk, begin managing all local privileged accounts (ex: local admins) on endpoints. (Local Security | Details Tab)

Local Security

Refer to the Local Security documentation pages to learn more about:

- Create & Manage Computer Groups, Local Groups, and Users

Application Control

Refer to the Application Control documentation pages to learn more about:

- Application Control - Policy & Config Overview / Collecting File Data
- Sending Policies to Endpoints - View Deployment Status / Update Using Powershell / Agent Event Log Viewer
- Event Discovery - Learning Mode Policies & Examples / View Policy Results

- Creating Policies - Allowlisting, Denylisting, Quarantine, Elevation, Greylisting, & Reputation Checking Examples
- Policy Priority Overview & Example

Integrations

Refer to the Integration documentation pages to learn more about:

- Integration & Foreign Systems

Reports & Troubleshooting

Refer to these documentation pages to learn more about:

- Reports
- Troubleshooting

Catalogs & Reference Guides

Refer to these documentation pages to learn more about:

- Policies Catalog
- Filters Catalog
- Actions Catalog
- Privilege Manager Glossary

Initial Login

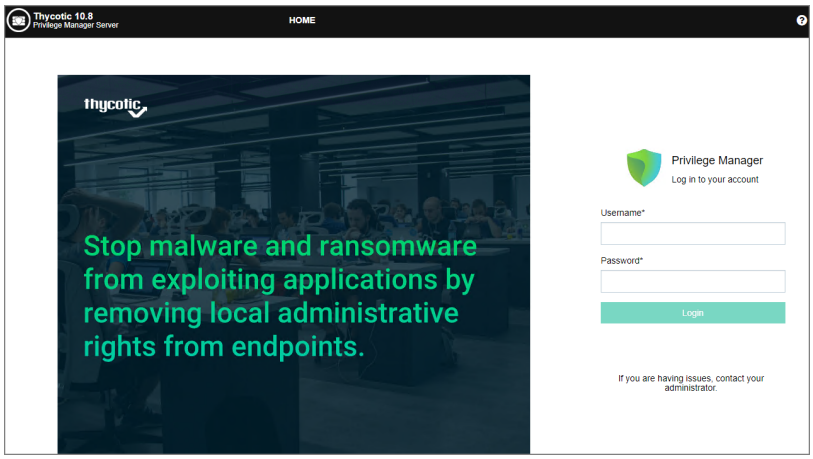
Using the credentials configured in the Create User section of the on-premises installation, validate that you can login to Privilege Manager and view the home screen.

The login URL for an on-premises Privilege Manager instance has this form:

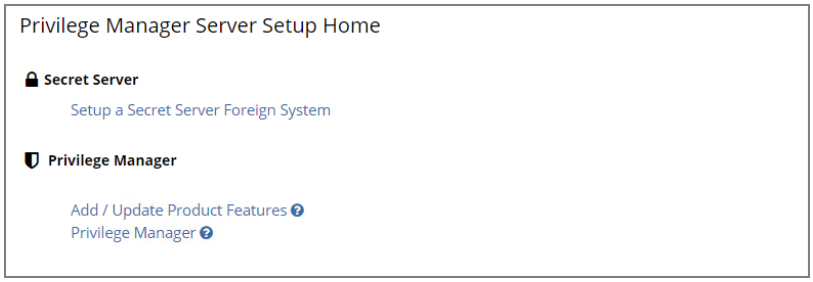
```
https://[server-domain]/TMS/PrivilegeManager
```

Note: On combined Secret ServerPrivilege Manager installations you are initially logged in throughSecret Server. If this is the case, you can find Privilege Manager by navigating to **Tools | Privilege Manager**.

The initial login for on-prem happens via NTLM.



After logging in the Privilege Manager Setup Home page opens.



Use the Privilege Manager link to login to the product. If you need to add or update product features, such as connectors for foreign systems, use the **Add / Update Product Features** link.

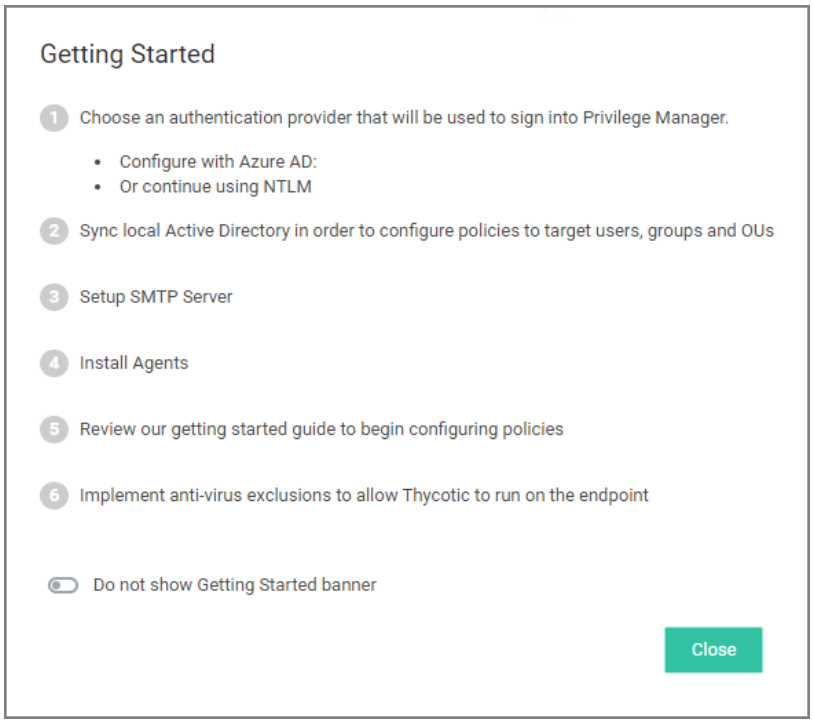
The **Setup a Secret Server Foreign System** link can be used to set-up an integration with Secret Server. This will also allow you to use Secret Server as an authentication provider. Also refer to Setting up Integration between Privilege Manager and Secret Server.

Getting Started Banner

At initial login the Getting Started Banner displays with help tips and next steps:

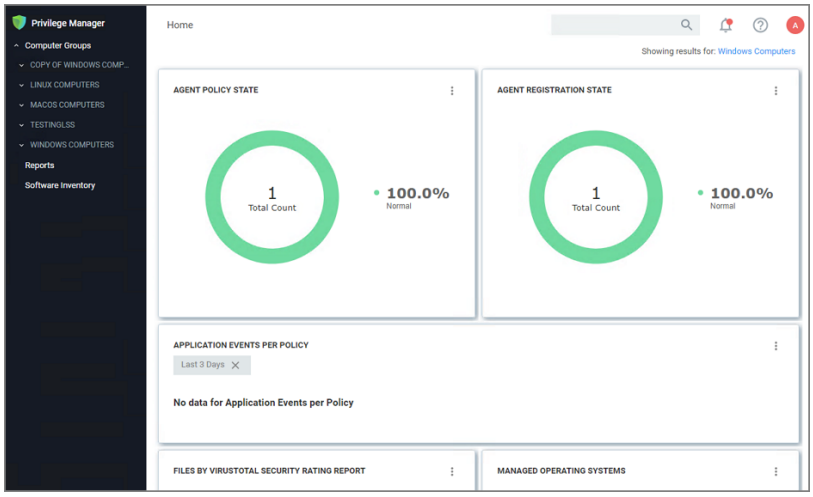
- Choose an authentication provider that will be used going forward to sign in to Privilege Manager.
- Setup the SMTP Server.
- Install Agents.
- Review the documentation to begin configuring policies.
- Implement anti-virus exclusions to allow Delinea to run on the endpoint.

You may choose to not show the Getting Started Banner on subsequent logins.



Home

The Home screen of Privilege Manager can be found by clicking Home in the top banner of any page inside of Privilege Manager. From this dashboard you can jump into either Application Control or Local Security, depending on what you want to do. You also will be given different snapshots of various important information about your environment. Once you have agents installed and policies setup, you'll have a lot going on from the Home Dashboard:



Getting Started Overview - Cloud

The following topics provide a guided path through the instance setup and subsequent initial sign-in steps of a cloud Privilege Manager instance.

- "Initial Setup - Cloud" on page 100
-
- "Privilege Manager Cloud Login" on the next page
- "Agent Installation" on page 61
  - "Setting the Privilege Manager Server Address" on page 208, if the address provided during the agent installation requires updates.

    Note: If you are targeting macOS based endpoints, refer to "Getting Started with macOS" on page 146.

Rollout Recommendation

Familiarize yourself with the concept. Delinea recommends a phased roll-out between the Application Control and Local Security, for example:

1. "Best Practice: Policy Feedback" on page 469: Set up learning mode policies on a group of test endpoints to learn about applications running on your endpoint machines ("Monitoring Policies (Learning Mode)" on page 256)
2. Local Security: Begin with "Local Security" on page 446 (only) and defining local group membership (Local Security | Manage Local Users)
3. Application Control: Tailor your policies so that they won't disrupt employee work ("Elevation Policies" on page 299) but will block known malicious applications (Creating Policies | Example: Quarantine Specified Malware). Implement these basic policies across agents in production
4. Application Control: Continue to tailor policies according to employee roles. Create a "Request Access" system for any unknown applications. ("Application Execution Requires Approval" on page 303 (Workflow))
5. Local Security: Once a workflow has been established between employees and the Privilege Manager Helpdesk, begin managing all local privileged accounts (ex: local admins) on endpoints. (Local Security | Details Tab)

Local Security

Refer to the Local Security documentation pages to learn more about:

- "Creating Computer Groups" on page 429

Application Control

Refer to the Application Control documentation pages to learn more about:

- "Application Policies" on page 230
- "Sending Policies to Workstations" on page 242

- "Monitoring Policies (Learning Mode)" on page 256
- "Example Policies" on page 279
- "Policy Priority" on page 269

Integrations

Refer to the Integration documentation pages to learn more about:

- "Foreign Systems" on page 569

Reports & Troubleshooting

Refer to these documentation pages to learn more about:

- "Reports" on page 884
- "Troubleshooting" on page 906

Catalogs & Reference Guides

Refer to these documentation pages to learn more about:

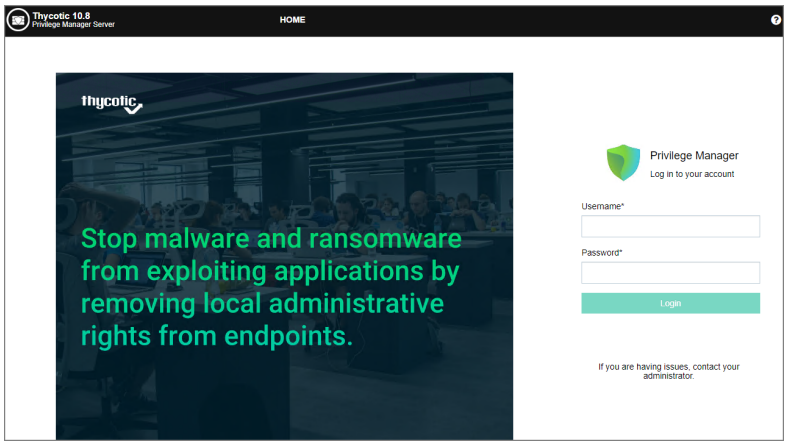
- "Application Policies" on page 230
- "Filters" on page 667
- "Actions" on page 495
- Privilege Manager"Glossary" on page 1022

Privilege Manager Cloud Login

To login to a Privilege Manager Cloud instance, use the URL and credentials provided to you. The URL is in the format of:

`https://myassignedname.privilegemanagercloud.com/Tms`

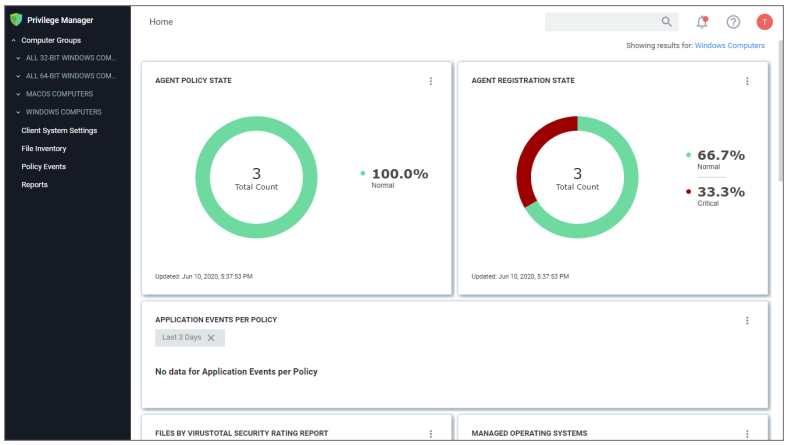
1. Navigate to your assigned login URL.



Depending on the authentication provider setup, users are presented with different login choices.

2. Click **Login** . This usually opens the Sign In dialog:
   a. Enter your username or email address and click **Next**.
   b. Enter your password and click **Login**.

   The Privilege Manager Cloud console home page opens:



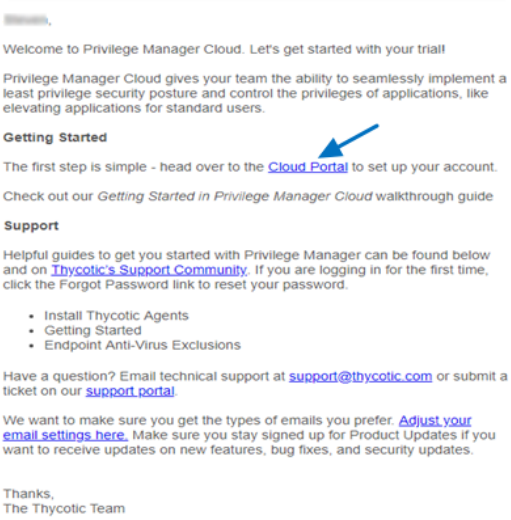
> **Note:** To import and synchronize Azure Active Directory Groups and Users, refer to the following topic: Setting Up Azure Active Directory Integration in Privilege Manager.

To addThycotic One# users manually, refer to the following topic: How to Add Thycotic One Users Manually. That topic does also cover how to create Standard and API Client users.

Initial Setup - Cloud

After you've signed up for a Privilege Manager Cloud trial, you will receive 2 emails. The first one is from Customer Support and will ask you to create a password to log into the customer support portal.

The second email you will receive is from Privilege Manager Sales titled Privilege Manager Cloud Trial. This email directs you to the **Cloud Portal** to begin your instance setup.



Welcome to Privilege Manager Cloud. Let's get started with your trial!

Privilege Manager Cloud gives your team the ability to seamlessly implement a least privilege security posture and control the privileges of applications, like elevating applications for standard users.

Getting Started

The first step is simple - head over to the Cloud Portal to set up your account.

Check out our *Getting Started in Privilege Manager Cloud* walkthrough guide

Support

Helpful guides to get you started with Privilege Manager can be found below and on Thycotic's Support Community. If you are logging in for the first time, click the Forgot Password link to reset your password.

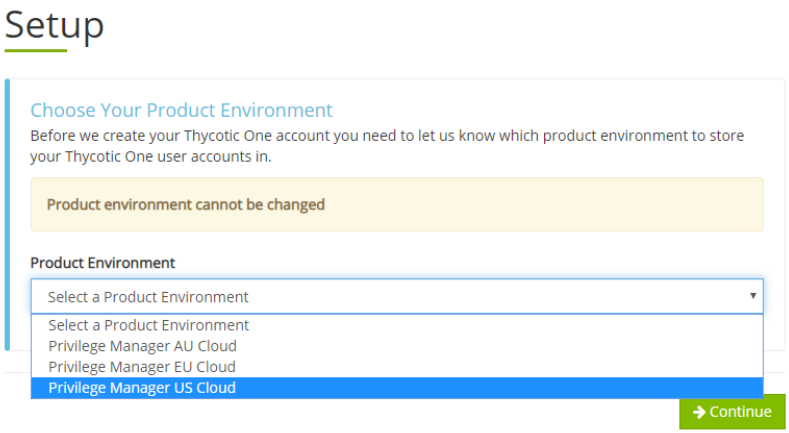
- Install Thycotic Agents
- Getting Started
- Endpoint Anti-Virus Exclusions

Have a question? Email technical support at support@thycotic.com or submit a ticket on our support portal.

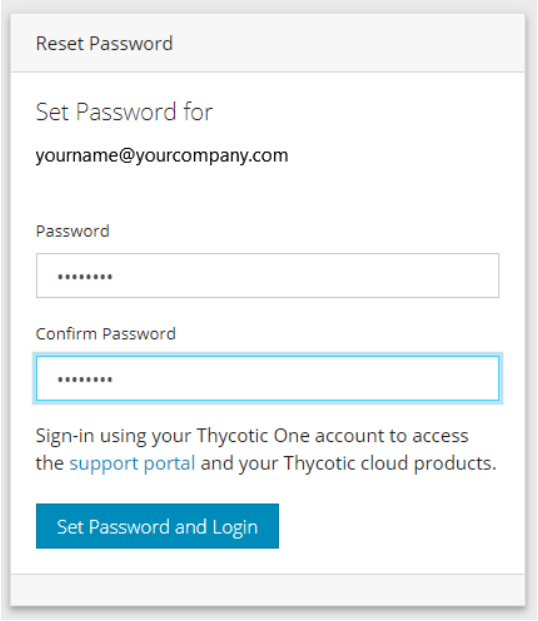
We want to make sure you get the types of emails you prefer. Adjust your email settings here. Make sure you stay signed up for Product Updates if you want to receive updates on new features, bug fixes, and security updates.

Thanks,
The Thycotic Team

Select the Cloud Portal link. On the Setup page, choose your Cloud Environment location from the drop-down menu. Then click **Continue**.

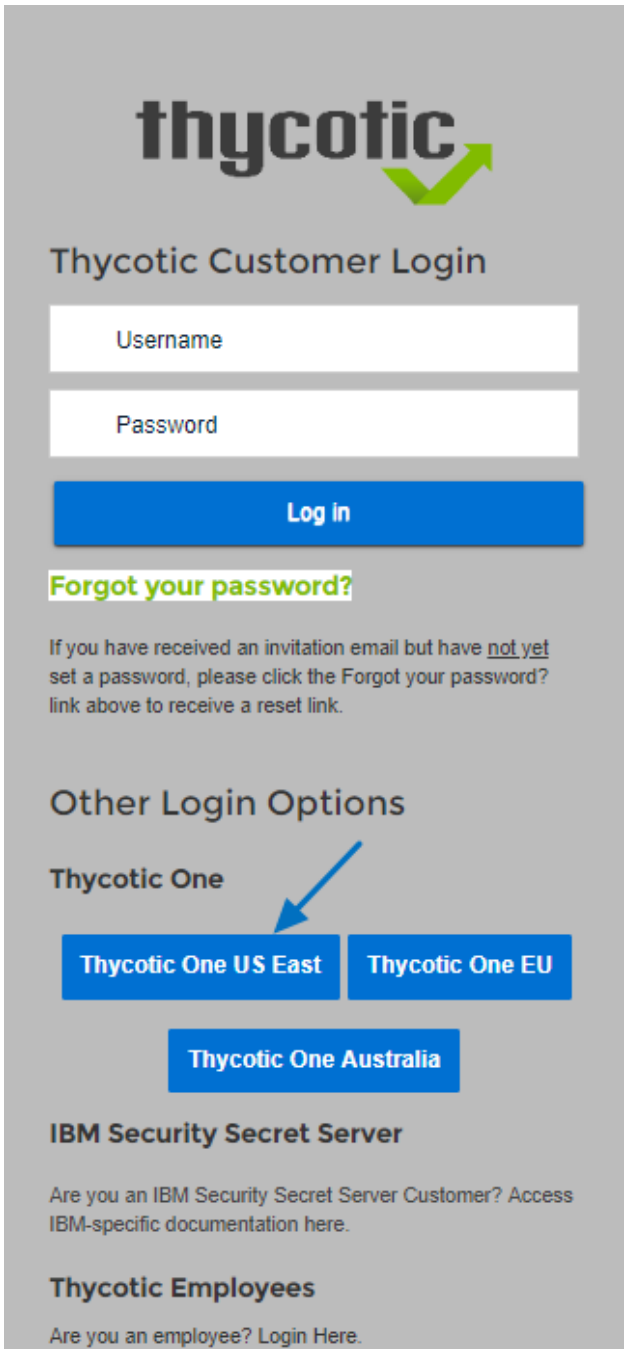


You will be directed to the Thycotic One portal to create the password for your first user account with Administrator credentials. This account will be assigned to the email address you entered to request the trial. After confirming the password, click **Set Password and Login**.

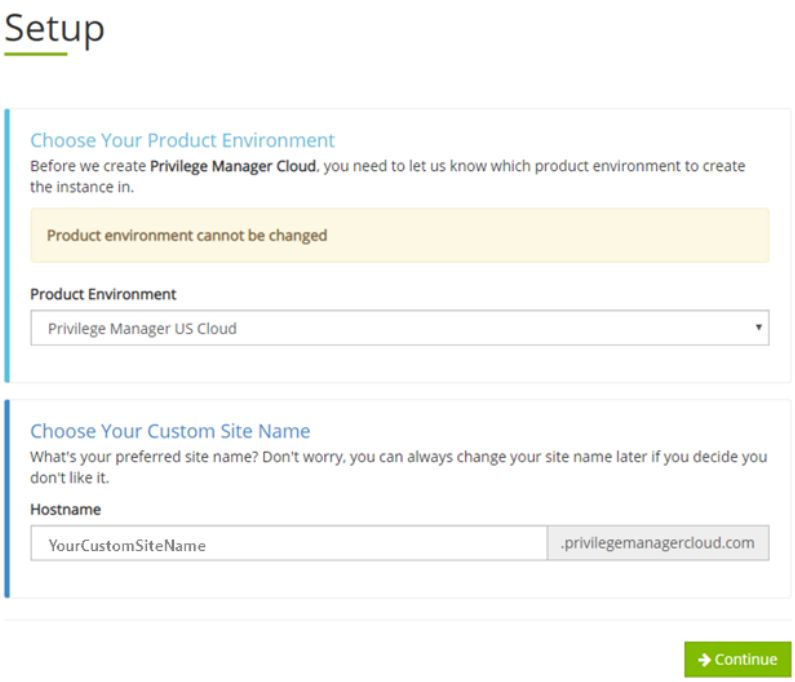


Important: Privilege Managerrecommends that you store the password in a secured physical location such as a safe or locked file cabinet. You can reset the password using an email reset, but **if this password is forgotten or you no longer have access to the email account, Privilege Manager will not be able to reset this password.**

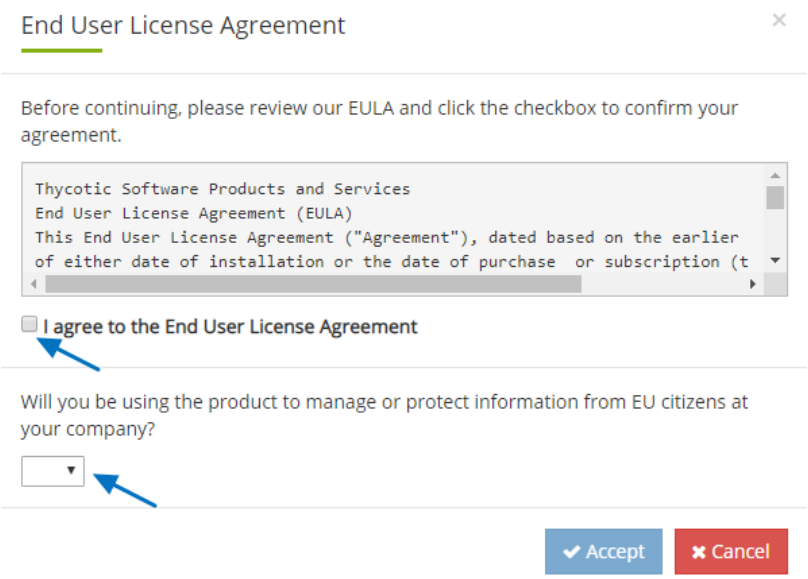
On the Privilege Manager Login page, click the blue button that corresponds to your new Cloud's Thycotic One location (chosen above).



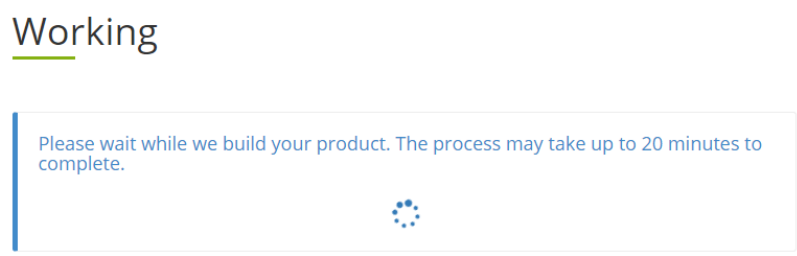
Next, on the Setup page choose the location of your cloud environment and enter the **Name** for your subdomain. Do not use special characters or spaces.



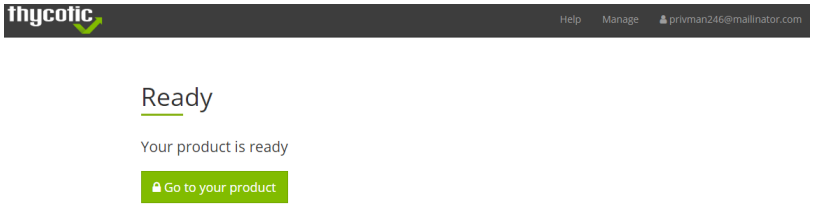
Read the End User License Agreement and click the box to signify agreement. From the drop-down, select Yes or No to signify your organization's oversight of EU information. Click **Accept**.



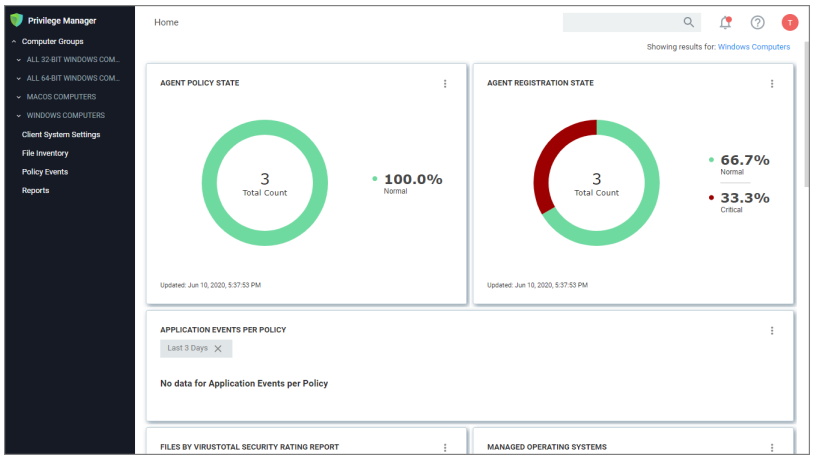
It will take approximately **20 minutes** for your new Privilege Manager Cloud to spin up.



When complete, click **Go to your Privilege Manager Cloud** instance and **Login with Thycotic One**.



You will be automatically redirected to your new Privilege Manager Home page.



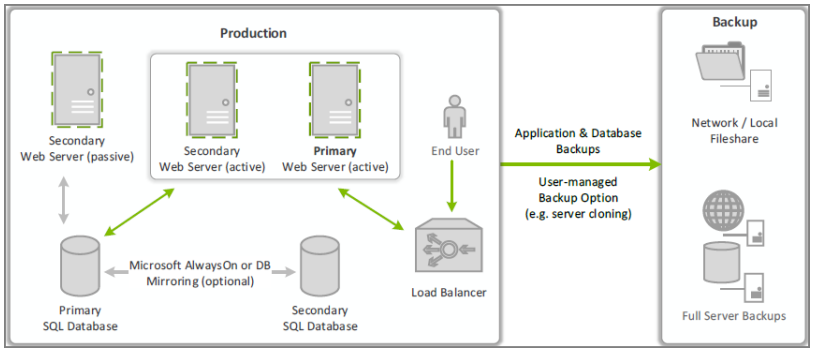
Setting Up Your Infrastructure

This sections contains topics around infrastructure set-up and/or changes:

- Setting up Internet Connected Clients
- Setup High Availability/Clustering
- Setup Reverse Proxy
- VM Deployments
- Migrating SQL Server Database for Privilege Manager and Secret Server Combined Installation
- Migrating the Privilege Manager Server
- Removing Privilege Manager from a Combined Install

Privilege Manager High Availability Setup

This topic explains the steps involved to set up DelineaPrivilege ManagerHigh Availability, also known as clustering.



Pre-requisites

Make sure that Privilege Manageris installed and working on a primary node with an existing database.

To cluster Privilege Managera secondary server must be prepared with the proper Privilege Managerpre-requisites. The pre-requisites check can be performed via standard Privilege Managersetup.exe. However, exit that automated installer once all pre-requisites clear.

Except for the Operating System, the following pre-requisites will be installed automatically by our installer. If you already have some of them installed or wish to install them yourself then the installer will skip over them.

System Requirements Overview

1. **Windows 2012 R2 or newer** operating system (2012 or newer is recommended)
2. Microsoft **SQL Server 2012 or newer** (Standard edition or higher is recommended)
3. Microsoft **Internet Information Services** (IIS) **7 or newer**
4. Microsoft **.NET Framework 4.6.1 or newer**

Note: Windows Server 2016 comes with the .NET Framework already installed.

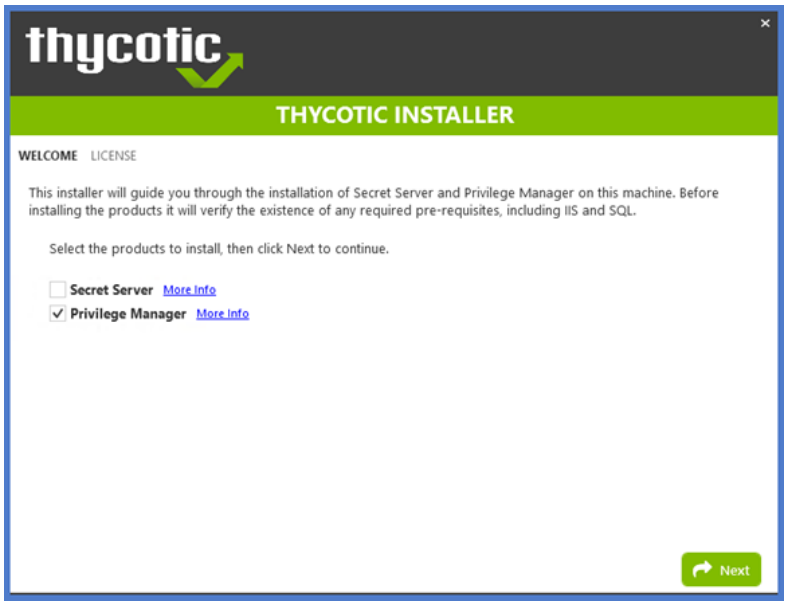
Using the Installer to Install/Confirm Pre-Requisites

The latest version of Privilege Manageris available for download. By clicking the Installer (.exe) link, a setup.exe file will be downloaded to your machine. It is recommended to run the setup.exe file as an administrator.

Note: The setup executable will ONLY be used to install/confirm all pre-requisites are installed on the web server. After confirming the pre-requisites, the installer will be closed and a manual installation will be completed. The manual installation will allow for separate databases and custom file locations. Do NOT complete the installation with the setup executable.

Running the setup.exe will begin an installation wizard. This wizard will ONLY be used to install any remaining pre-requisites required on the web server. The wizard will walk through the initial installation steps, beginning with a Welcome page.

1. On the Welcome dialog, verify that Privilege Manageris selected and select the checkbox if not already checked.



2. Click **Next**.
3. On the License dialog review the End User License Agreement (EULA) and click **Accept License**.
4. On the Database dialog select **Connect to an existing SQL Server**, click **Next**.
5. The Pre-Requisites dialog helps you to ensure everything that is required gets installed for Privilege Manager. Click **Fix Issues** to automatically install the necessary pre-requisites.
6. Close the installer once all pre-requisites are successfully installed.

Note: Do NOT continue installing the products with this installer.

Manual Set-up of Secondary Node

In this procedure you will:

1. Copy the web application files from the primary server to the secondary server.
2. Use those copied files to setup and configure the secondary Privilege Managerserver.
3. Use the Internet Information Services Manager to setup Application Pools.
4. Convert application pools to applications.
5. Configure Authentication.
6. Set the Preload Status.
7. Change the Disable Overlapped Recycle setting.
8. Edit the TMS/Worker Web.config file.

Copy Web Application Files from Primary to Secondary Servers

1. On the primary server, decrypt the **connectionStrings.config** by running the following command:

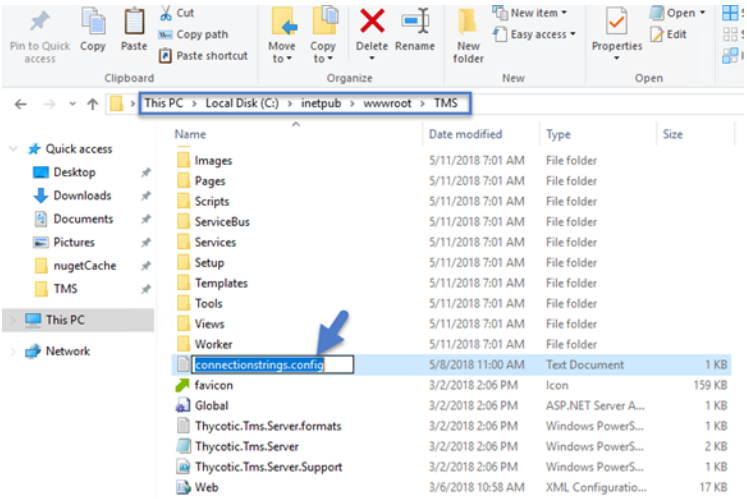
```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pd
"connectionStrings" -app "/Tms"
```

2. Select and copy all contents of the Privilege Managerweb application folder at

```
C:\inetpub\wwwroot\TMS\
```

   Including the unencrypted connectionStrings.config file.

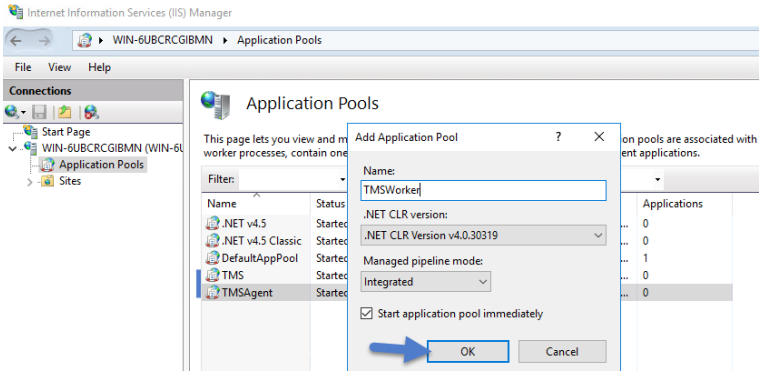
3. On the secondary server, create the same folder path.
4. Paste the entire contents of the Privilege Managerweb application folder from the primary web server to the similar location on the secondary web server.



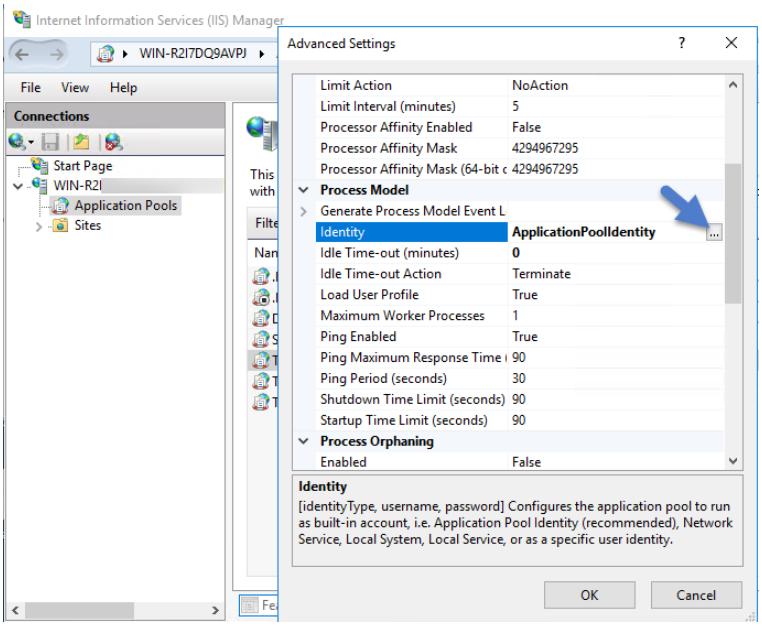
Setting up Application Pools

1. Open **Internet Information Services Manager** (inetmgr).
2. Under your local server, right-click **Application Pools** and select **Add Application Pool...**
3. **Add** three new application pools.
   a. **TMS** - Under General > Start Mode select **OnDemand (Default)**.
   b. **TMSAgent** - Under General > Start Mode select **AlwaysRunning**.

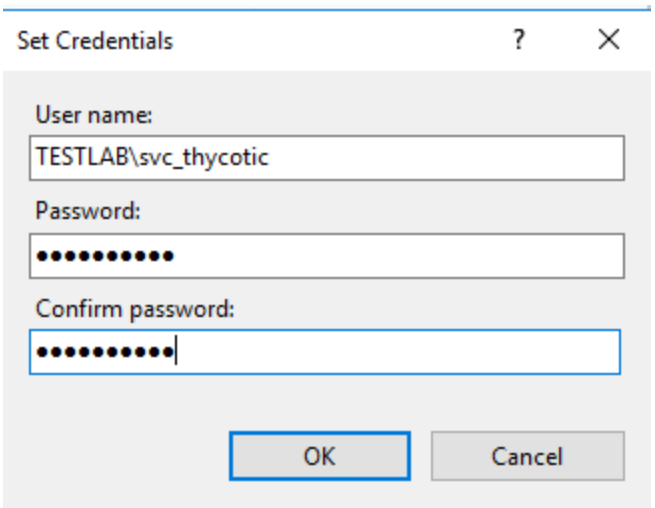
c. **TMSWorker** - Under General > Start Mode select **AlwaysRunning**.



4. For each of the 3 app pools (TMS, TMSAgent, and TMSWorker),
   a. right-click on each app pool,
   b. select **Advanced Settings...**
   c. then the **Identity** box in the "Process Model" section,
   d. click the three dots on the right of the box.



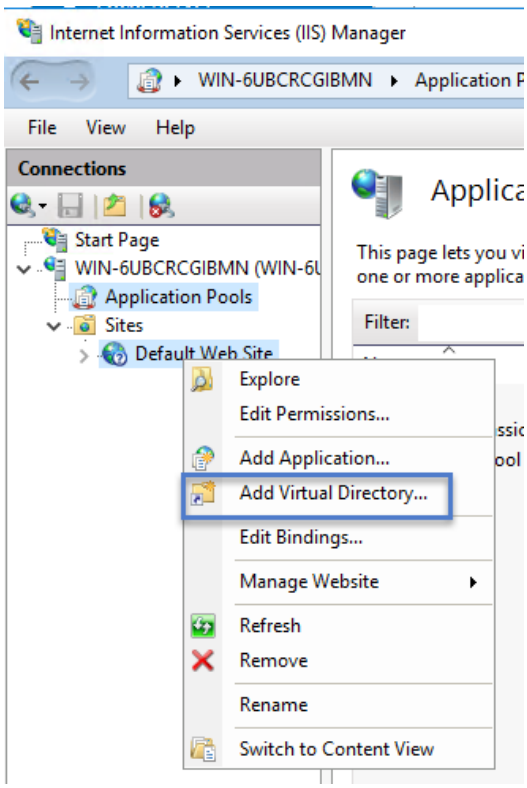
   e. Select the **Custom Account** radio button,
   f. Click **Set**, enter your service account's name and password.



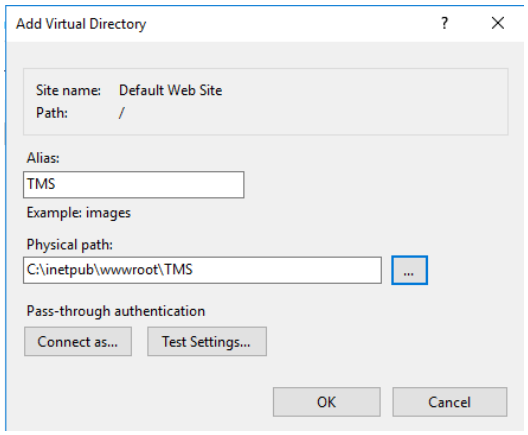
g. Click **OK**.

Converting the Application Pools

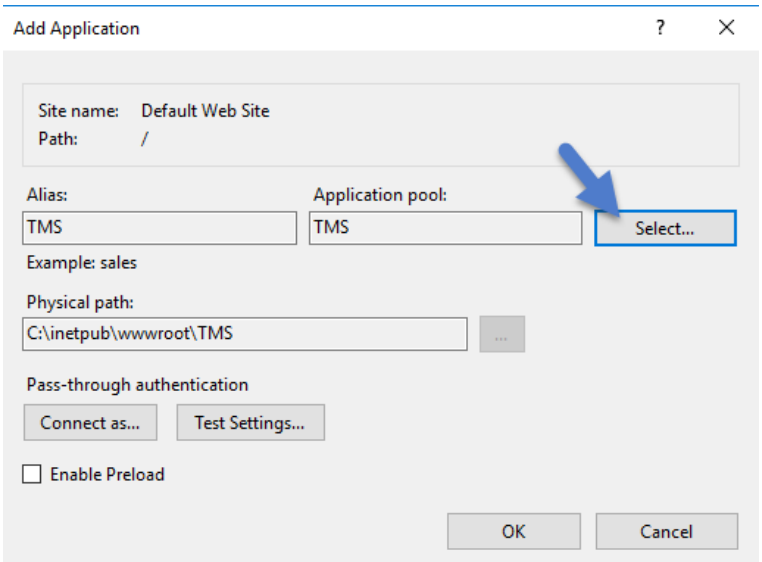
1. Right-click **Default Web Site** in IIS and select **Add Virtual Directory...**.



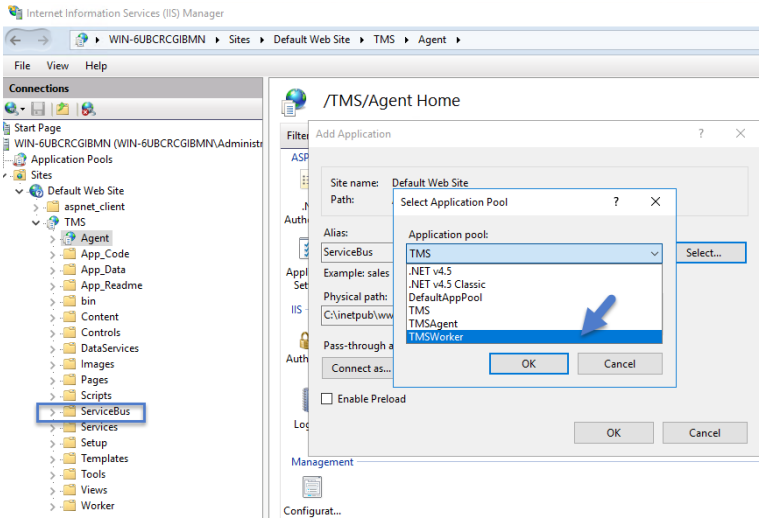
2. Select an alias for your Privilege Manager. The alias is what will be appended to the website. For instance, "TMS" in `http://myserver/TMS`.
3. Next, enter the physical directory where you unzipped Privilege Manager(i.e., 'C:\inetpub\wwwroot\TMS').



4. Click **OK**.
5. In the tree, right-click the new virtual directory and select **Convert to Application**.
   a. Set the **Application Pool** to the one called **TMS**.
   b. Click **OK**.



6. In the virtual directory expand the new **TMS** site,
   a. right click the **Agent** Subfolder and select **Convert to Application**.
   b. Set the **Application Pool** to the one called **TMSAgent**, click **OK**.
7. In the virtual directory navigate to the **ServiceBus** Subfolder.
   a. Right-click and select **Convert to Application**.
   b. Set the **Application Pool** to the one called **TMSWorker** you created earlier, click **OK**.

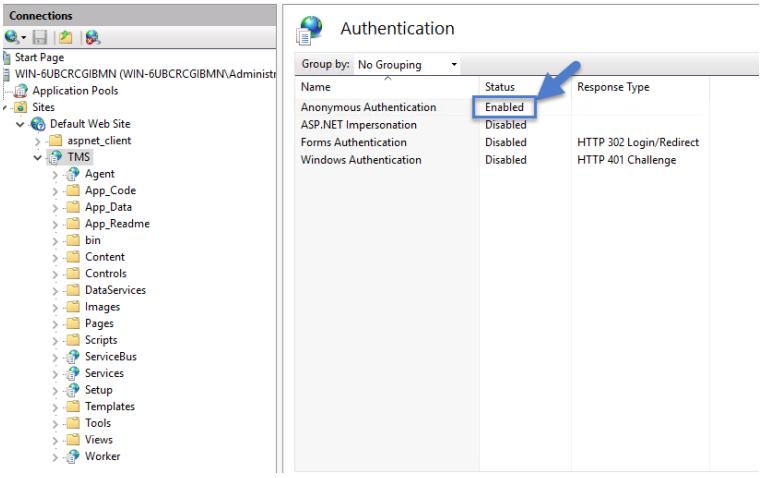


8. In the virtual directory select the **Services** Subfolder,
   a. Right-click the new virtual directory and select **Convert to Application**.
   b. Ensure that the **Application Pool** is set to the one called **TMS**, click **OK**.
9. In the virtual directory select the **Setup** Subfolder,
   a. Right-click the new virtual directory and select **Convert to Application**.
   b. Ensure that the **Application Pool** is set to the one called **TMS**, click **OK**.
10. In the virtual directory select the **Worker** Subfolder,
    a. Right-click the new virtual directory and select **Convert to Application**.
    b. Set the **Application Pool** to the one called **TMSWorker**, click **OK**.

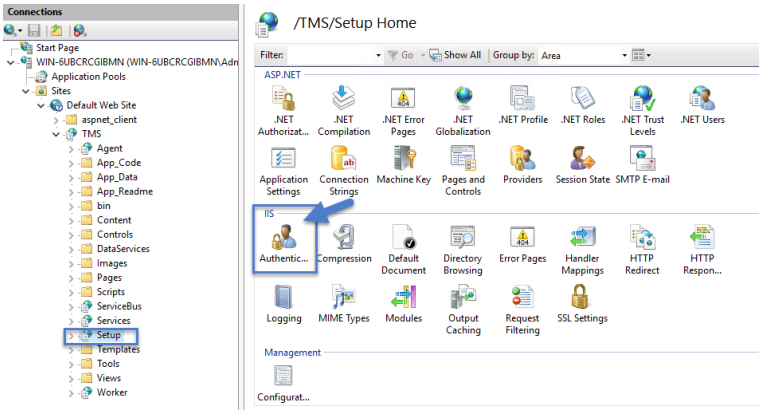
Setting Authentication

1. Select your **TMS** virtual directory.
   a. Double-click **Authentication** in the features pane.
   b. Make sure that only **Anonymous Authentication** is set to **Enabled**. Everything else should be set to

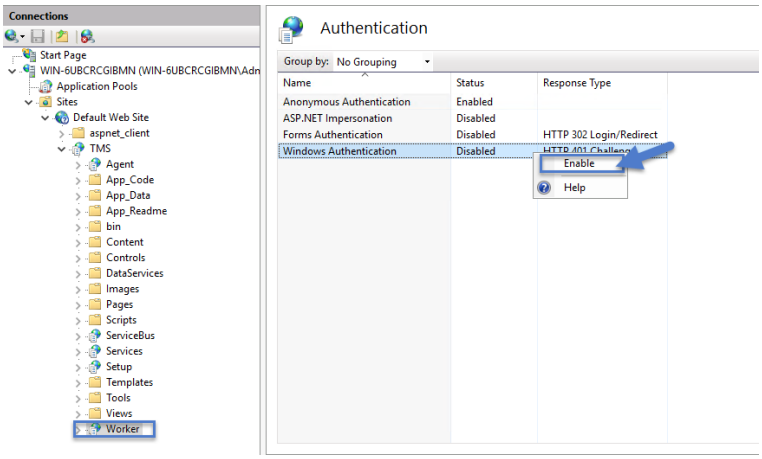
disabled.



2. Select the **Setup** directory.
   a. Double click **Authentication** in the features pane.
   b. Make sure that **Anonymous Authentication** and **Windows Authentication** are both set to **Enabled** and everything else is disabled.

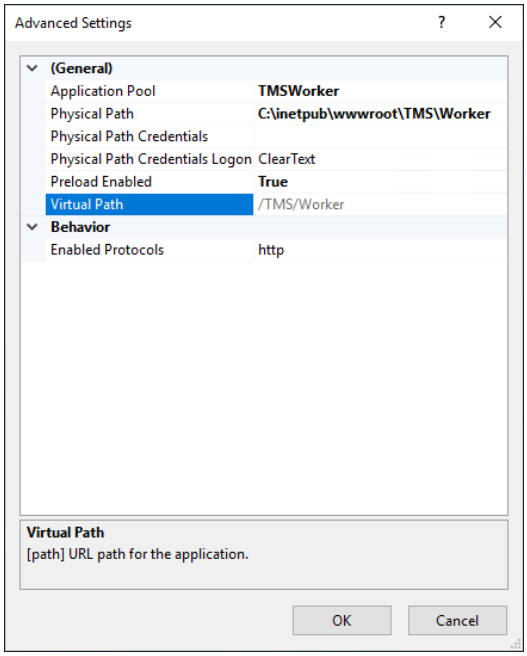


3. Select the **Worker**.
   a. Double-click **Authentication** in the features pane and make sure that **Anonymous Authentication** and **Windows Authentication** are both set to **Enabled** and everything else is disabled.



Setting the Preload Status

1. Right-click the **TMSWorker** application.
2. Select **Advanced** settings.
3. Under **General** > **Preload Enabled**, change the setting to **True**.

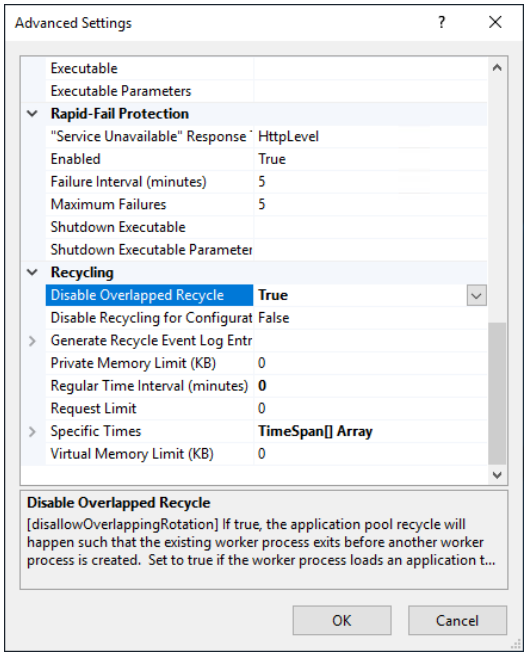


HA Deployment

Perform the following IIS changes as part of the best practices setup.

1. In IIS, right-click the **TMSWorker** application pool.
2. Select **Advanced Settings**.

3. Under the **Recycling** section, change **Disable Overlapped Recycle** to **True**.



4. Navigate to `C:\inetpub\wwwroot\TMS\Worker\Web.config`.
5. Locate the **system.webServer** section and add:

```
<applicationInitialization doAppInitAfterRestart="true">
    <add initializationPage="/status/ping" /> </applicationInitialization>
```

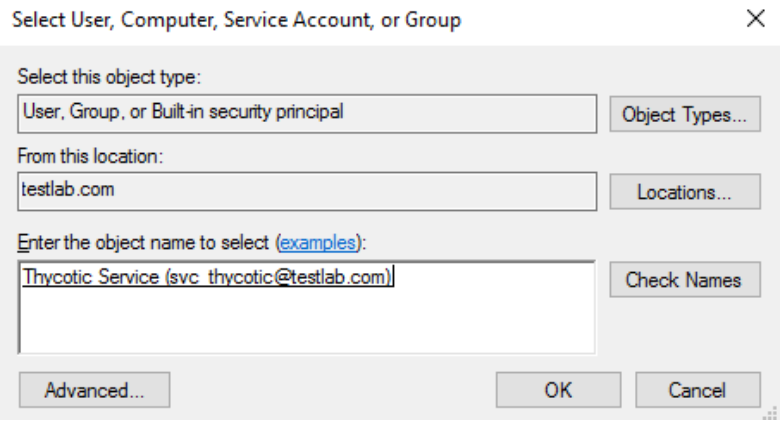
The section should now look like this:

```
<system.webServer>
    <applicationInitialization doAppInitAfterRestart="true">         <add
initializationPage="/status/ping" />     </applicationInitialization>      <modules
runAllManagedModulesForAllRequests="true">         <remove
name="UrlRoutingModule"/>         <add name="UrlRoutingModule"
type="System.Web.Routing.UrlRoutingModule, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a"/>     </modules>     <handlers>         <add
name="UrlRoutingHandler" preCondition="integratedMode" verb="*"
path="UrlRouting.axd"             type="System.Web.HttpForbiddenHandler, System.Web,
Version=2.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a"/>     </handlers>     <security>         <authorizatio
n>             <add accessType="Allow"
users="?"/>         </authorization>     </security> </system.webServer>
```

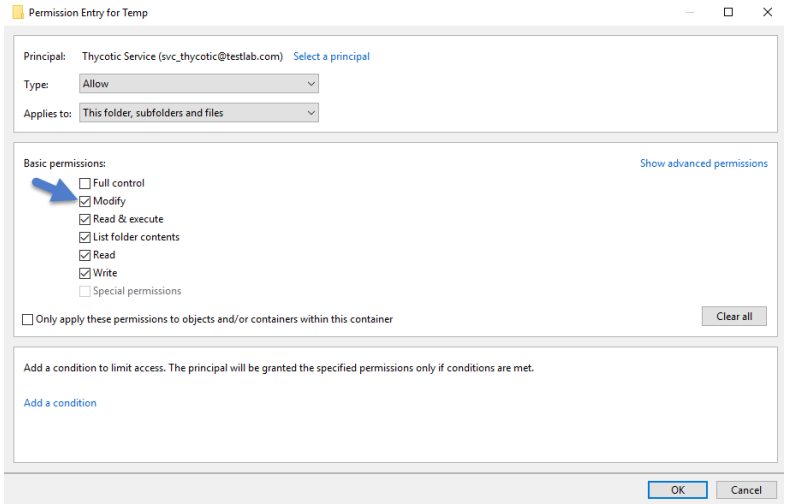
Folder Permissions to C:\Windows\Temp

1. Navigate to the **C:\Windows\TEMP** folder.
2. Right-click the folder and select Properties | Security | Advanced.

3. Click **Add** and **Select a principal**.
4. Ensure the domain machine is listed as the **Location** and type the service account into the **Enter the object name to select** field.
5. Click **Check Names** and **Enter network credentials** for accessing your domain machine.



6. Click **OK**.
7. Under Basic permissions, select the **Modify** checkbox.

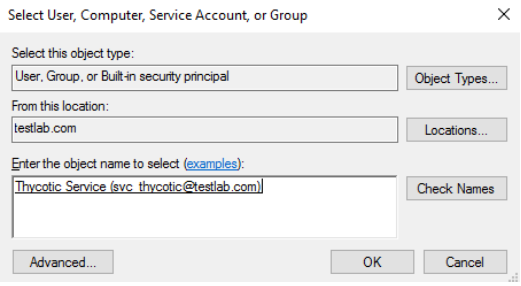


8. Verify your service account has **Modify**, **Read & execute**, **List folder contents**, **Read**, and **Write** permissions for the **C:\Windows\TEMP** folder.
9. Click **OK**, then **Apply**.

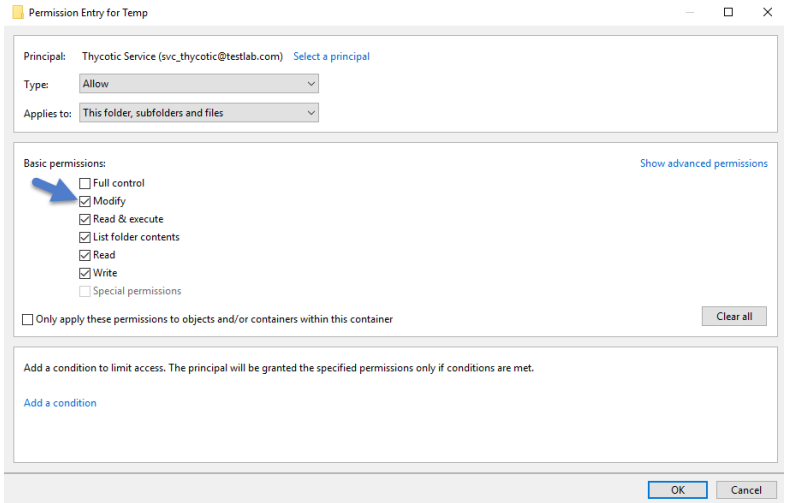
Folder Permissions to the Privilege ManagerApplication Folder

1. Navigate to the Privilege Managerapplication folder at **C:\inetpub\wwwroot\TMS**.
2. Right-click the folder and select Properties | Security | Advanced.
3. Select **principal**.

4. Ensure the domain machine is listed as the **Location** and type the service account into the **Enter the object name to select** field.
5. Click **Check Names** and **Enter network credentials** for accessing your domain machine.



6. Click **OK**.
7. Under Basic permissions, select the **Modify** checkbox.



8. Verify your service account has **Modify**, **Read & execute**, **List folder contents**, **Read**, and **Write** permissions for the **C:\Windows\TEMP** folder.
9. Click **OK**, then **Apply**.

> **Note:** The application folder only needs **Write** and **Modify** permissions during the installation or during an upgrade. You can remove these once the installation process is complete.

Upgrade Prep

Following these changes, ensure that

- all server nodes are up and running without error conditions.
- all server nodes have access to the NuGet repository.
- for upgrades login into one of the server nodes directly and not the clustered shared address.
- Initiate the upgrade, the selected node will deploy all upgrade components to all other nodes within the cluster.

Permission to Certificate Private Key (prior to 10.6 only)

Note: This is only required for Privilege Managerprior to release 10.6.

TMS requires **Read** access to the private key of the certificate being used for the HTTPS binding. To set this:

1. Open **mmc.exe** as an administrator.
2. Add the certificate manager snap-in choosing to manage certificates for the computer account (**File | Add/Remove Snap-in…**)
3. Click **Certificates**,
4. then **Add | Computer account | Next | Local computer | Finish | OK**.
5. Find the certificate that the HTTPS binding for your site is using.
6. Right-click on the certificate and select **All Tasks | Manage Private Keys**.
7. Grant **Read** access to the identity account for your application pools.

If the "Manage Private Keys" option is not available, you can set this permission in PowerShell.

Verify Login on Secondary Node

1. Navigate to Privilege Manager, ex: **http://localhost/TMS**. You should be able to authenticate to Privilege Manager.
2. After logging in, all policies and all data accessible on the primary node should be accessible on the secondary node.

Re-encrypt ConnectionStrings.config

1. On the **primary node**, run the following command to re-encrypt the connectionStrings.config file:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pe
"connectionStrings" -app "/Tms"
```

2. On the **secondary node**, run the same command to re-encrypt the connectionStrings.config file:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pe
"connectionStrings" -app "/Tms"
```

Privilege Managerhas now successfully been clustered. A load balancer, GTM, VIP, etc. can be used to manage the traffic. The settings to configure this will be handled on the side of this infrastructure piece and is beyond the scope of this document. Contact Delinea's Professional Services team if additional consultation is required.

Delinea requires that **sticky sessions** are enabled on the load balancer to prevent a user from bouncing between servers on each request of a single session.

Setting Up Your Infrastructure

This sections contains topics around infrastructure set-up and/or changes:

- Setting up Internet Connected Clients
- Setup High Availability/Clustering
- Setup Reverse Proxy
- VM Deployments
- Migrating SQL Server Database for Privilege Manager and Secret Server Combined Installation
- Migrating the Privilege Manager Server
- Removing Privilege Manager from a Combined Install

Migrating SQL Server Database for Privilege Manager and Secret Server Combined Installation

If you have a combined installation of Privilege Manager and Secret Server and wish to move/migrate the MS SQL Server databases, follow the steps below for the case that applies to you:

- **Case I**: Keeping all data in the current database: Backup the existing databases and restore them to the new SQL Server using the instructions below:
  - For Privilege Manager: see Moving the Privilege Manager DB topic below.
  - For Secret Server: Moving the Microsoft SQL Server Database to Another Machine.

  If you have successfully performed the backup and restore (per the applicable instructions above), your site will be connected to the new database.
- **Case II**: Abandoning all data and starting fresh:
  1. In Privilege Manager, go to `https://<SERVERNAME>/Tms/Setup/Database/ConnectDatabase`
  2. Provide the new database connection and click **OK**
  3. Install desired Delinea products like Privilege Manager and/or Secret Server.

Moving the Privilege Manager DB

Step 1: Backup and Restore the Database

1. Stop the TMS site (Ams site for Arellia) in Internet Information Server (IIS) to prevent any changes to the database
2. Stop the TMS, TMSAgent, and TMSWorker application pools (Ams and AmsWorker application pools for Arellia).
3. Back up the database by accessing SQL Management Studio and right-clicking on the database to select Tasks > Back Up.
4. Select a file location for the .bak file. Transfer this file to the new server.
5. On the new database server, through SQL Management Studio, restore the database backup (the .bak file).

6. Create and/or grant access to the account that will be accessing the database (see TMS Installation Guide for account creation instructions)

We recommend taking the old database offline.

Step 2: Connect to the new database (configure the database connection details)

1. Restart TMS website.
2. Check that the TMS, TMSAgent, and TMSWorker application pools are running.
3. Browse to your TMS URL database connection page e.g. `https://<YOUR_URL_INSTANCE>/TMS/setup/database/connectdatabase` (for Arellia this URL would be slightly different e.g. `https://<YOUR_URL_INSTANCE>/ams/setup/database/connectdatabase`) and you will see a page to enter your new database connection details.

   Note: This can only be accessed locally via the server running the Privilege Manager instance or via active RDP session into the Privilege Manager server.
4. Enter your new SQL Server and the account information.
5. Click Next and the site will connect to the new database.

Your site is now pointing to the new database.

If also migrating to new web servers or doing a reinstallation, copy the tmsEncryption.config file(s) to the new web servers(s). The file is located on the web server at the root of the TMS web site and should be copied to the same place on the destination server(s): `\inetpub\wwwroot\TMS` This file is only applicable if current servers are on version 10.5 or higher. (refer to Item Encryption)

To roll back changes and restore the original database, simply start back at Step 1 and move the database back to the original database server.

Migrating the Privilege Manager Server

If you are moving/migrating Privilege Manager to a new machine and have installed IIS and .NET Framework as described in the Installation Guide on the new machine, you do not need to run the installer, simply follow the steps below:

1. Copy the folder that holds your Privilege Manager instance to the new computer.
2. Shut down the old web site and recycle its application pool as it is running background threads which are accessing the database.
3. Set up the new folder in Internet Information Server (IIS) as a virtual directory/application under the Default Web Site or as a separate Website (refer to the Advanced Installation section of the Installation Guide for detailed instructions).
4. Browse to your TMS URL database connection page e.g. `https://<YOUR_URL_INSTANCE>/TMS/setup/database/connectdatabase` (for Arellia this URL would be slightly different e.g. `https://<YOUR_URL_INSTANCE>/ams/setup/database/connectdatabase`) and you will see a page to enter your database connection details.
5. Activate the licenses for the new server by going to the Licenses page.

6. If you are using certs, remember to set them on your new IIS, then browse to Privilege Manager over HTTPS and re-enable force HTTPS if this was set on the original machine.
7. Re-enable DPAPI if this was disabled in the earlier step.

Note: If you're migrating the Privilege Manager web application from Windows Server 2008 to 2012 or newer AND your Privilege Manager is below version 8.5, make sure that:

- .Net extensions 3.5 and ASP.Net 3.5 when adding the IIS role on the new server.
- Change the Privilege Manager Application Pool to 2.0 and recycle the application pool after running the installer.

Steps to Setup Secondary Node with both Secret Server & Privilege Manager

If you are migrating a combined install environment, also perform these steps:

1. Check web-auth.config and web-cookie.config (in Secret Server web folder) to make sure forceSSL = 'false'.
2. Confirm app pool account and IIS settings (confirm if SS and TMS are virtual directories, confirm IIS auth settings).
3. Disable DPAPI.
4. Disable Force SSL.
5. Decrypt connectionStrings.config on primary web server:

   ```
   C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pd "connectionStrings" -app "/Tms"
   ```
6. Copy files to secondary.
7. Download current installer to secondary server.
8. Run installer to **confirm and fix pre-requisites only**. **DO NOT install the application** with the installer.
9. Make sure Secret Server and TMS web folders from primary are in `C:\inetpub\wwwroot` (or a similar location).
10. Create 4 app pools: SecretServer, TMS, TMSAgent, and TMSWorker (same as set for primary node).
11. Assign service account to all 4 app pools (same as set for primary node).
12. If the Secret Server and TMS directories do not appear in IIS Manager, add the virual directories (same as set for primary).
13. Convert to Applications
    a. Right-click on **Secret Server > Convert to Application**, make sure SecretServer app pool is assigned.
    b. Right-click on **TMS > Convert to Application**, make sure TMS app pool is used.
    c. Under TMS, right-click on **Agent > Convert to Application**, make sure TMSAgent app pool is used.
    d. Under TMS, right-click on **ServiceBus > Convert to Application**, make sure TMSWorker app pool is used.
    e. Under TMS, right-click on **Services > Convert to Application**, make sure TMS app pool is used.
    f. Under TMS, right-click on **Setup > Convert to Application**, make sure TMS app pool is used.
    g. Under TMS, right-click on **Worker > Convert to Application**, make sure TMSWorker app pool is used.

14. Run the ASP.NET IIS Registration Tool:
    a. Change the directory to your .NET framework installation directory using the "cd" command (i.e.: `C:\Windows\Microsoft.NET\Framework\v4.0.30319` or `C:\Windows\Microsoft.NET\Framework64\v4.0.30319`).
    b. Type in `.\aspnet_regiis -ga <domain name>\<user name>` and press enter.
15. Assign folder permissions:
    a. Give your service account "modify" access to `C:\Windows\TEMP`.
    b. Give your service account "modify" access to the Secret Server web folder.
    c. Give your service account "modify" access to the TMS web folder.
16. Set IIS authentications (set to same as primary, depending on IWA and other settings), typical example:
    - Secret Server (Anonymous & Forms, except winauthwebservices = Forms & Windows; see TMS notes)
17. Install certfification on new server, if not already done.
18. Give the 3 TMS App Pools read access on the PrivateKey of the cert.
    a. MMC snap-in > Certificates.
    b. Find the certificate (most like in personal store).
    c. Right-click > All Tasks > Manage PrivateKey.
    d. Choose local computer name from location and format is iis apppool\tms, iis apppool\tmsagent, iis apppool\tmsworker.
19. Login in to Secret Server.
20. Activate licenses.
21. Re-enabled Force SSL.
22. Re-enabled DPAPI on all web nodes.
23. Re-encrypt connectionStrings.config on all web nodes:

    ```
    C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pe "connectionStrings" -app "/Tms"
    ```

Setting up Internet Connected Clients

On-premises Privilege Manager instances need to use an Azure Service Bus for internet connected clients. The Azure Service Bus is a subscription service that external agents can connect to and use to communicate with an internal Privilege Manager Server (TMS) instance.

Note: Cloud customers don't need to use the Internet Connected Clients set-up, because their clients can already connect to the internet-based cloud instance.

With Privilege Manager 10.7 and up, TLS 1.2 is supported.

This page is broken up into three sections:

- Azure Service Bus Queue Configuration
- Setting up the Service Bus as a Foreign System in Privilege Manager

- Configuring the Agents to use the Service Bus (if this is a new agent installation, the Agents can be pointed directly at the Service Bus namespace URL)

Azure Service Bus Queue Configuration

Delinea requires a Service Bus relay for remote communication. For this a Service Bus Queue needs to be created, follow the procedure as outlined by Microsoft here in Quickstart: Use Azure portal to create a Service Bus queue.

1. In the Azure Service Bus portal go to the **Shared access policies** page.
2. Find the policy called **RootManageSharedAccessKey**. If you don't have one yet, create one by that name and select the **Manage** option and save it.
3. On the **RootManageSharedAccessKey** policy you can see the **Primary Key** field. Make note of where this is. We have use it in a step down below.
4. Next, navigate to the **Queues** page and create a new queue.
5. Do not check any of the options, using the defaults is fine. Take note of the queue name you gave it.

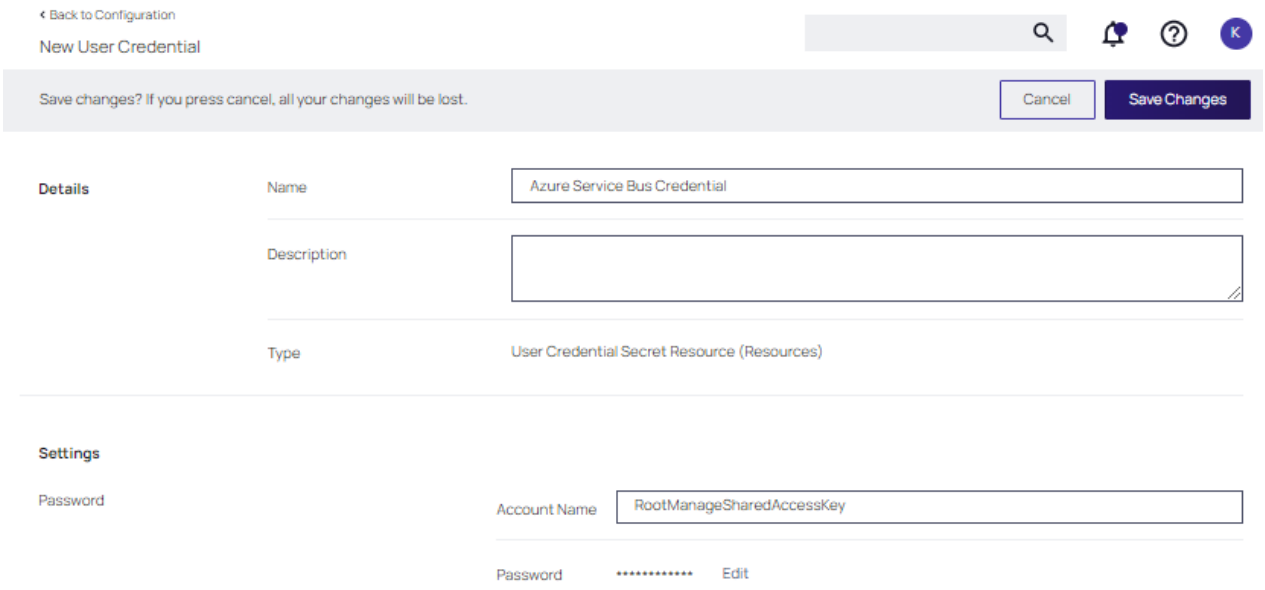
Next you will need to follow the instructions below to create a credential for the Service Bus and add the Service Bus as a foreign system in Privilege Manager.

Setting up the Service Bus Foreign System

The Azure Service Bus requires a Foreign Systems configuration in Privilege Manager. To configure a Service Bus instance with a custom URL and credentials follow these steps:

1. In the DelineaPrivilege Manager Console, click **Admin | Configuration**.
2. Click the **User Credentials** tab.
3. Click **Create**.

a. Enter a **Name**, for example *Azure Service Bus Credential*.

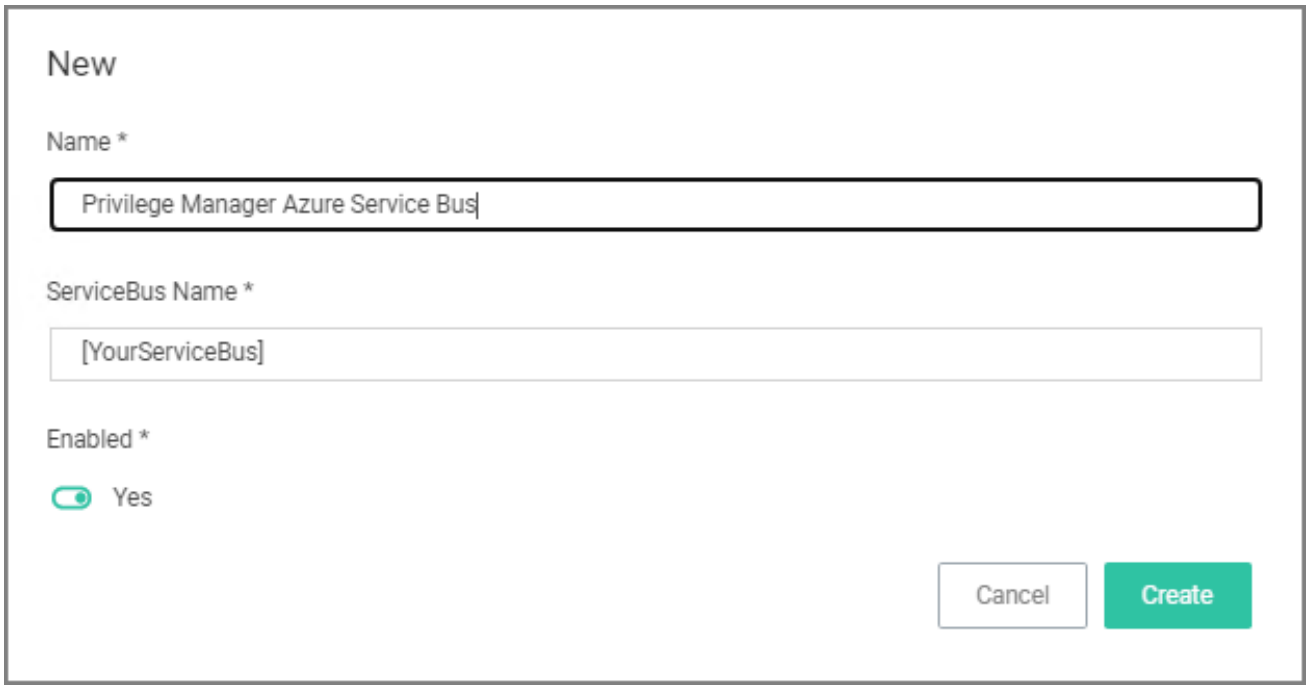


b. Set the Account name to **RootManageSharedAccessKey**.

c. Set the Password to the value of the **Primary Key** obtained during the Azure Service Bus configuration procedure **step 3** under "Azure Service Bus Queue Configuration" above.

d. Click **Save Changes**.

4. Navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
5. Click the **Azure Service Bus** option.
6. Click **Create**.

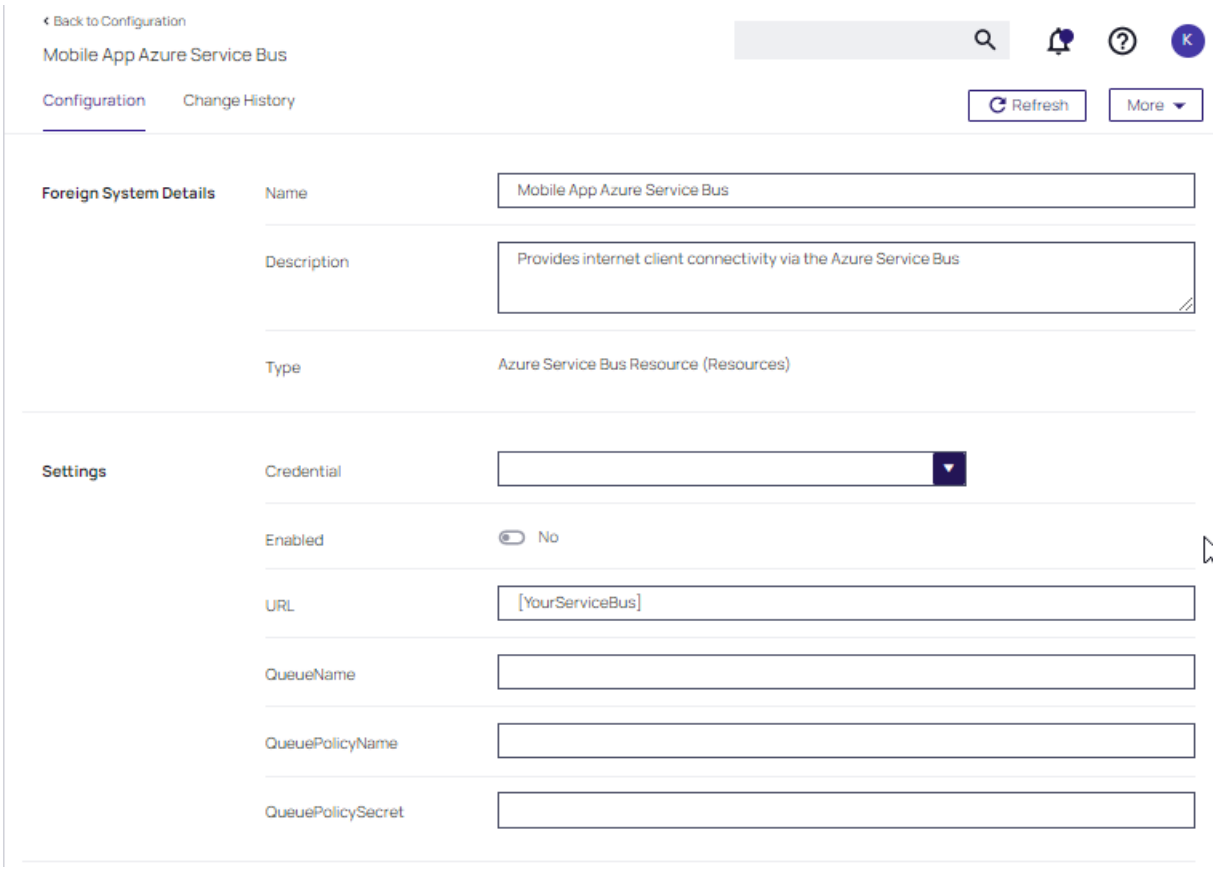


a. Enter a **Name**, for example *Privilege Manager Azure Service Bus*.

b. Set the **ServiceBus Name** to the namespace of the Service Bus from the Azure Portal. To find this value, open the Azure Portal, locate the Service Bus that is being used for this integration (refer to the intro above). Go to the **Properties** page and locate the Name property (generally, this is the same name as the instance you just located in the list of Service Bus instances).

c. Set the **Enabled** switch to **No** for now.

d. Click **Create**.



e. Set the credential to the credential created in step 3 of this procedure (*Azure Service Bus Credential*).

f. Leave the URL field as is (and ignore the fact that it's called URL – it's just the Service Bus name).

g. Make sure the URI matches the first part of the namespace created in Azure.

h. Set the QueueName to the same queue name created above in **step 4** under "Azure Service Bus Queue Configuration".

i. Set the Queue Policy Name to **RootManageSharedAccessKey**.

j. Set the Queue Policy Secret to the **Primary Key** as obtained in **step 3** under "Azure Service Bus Queue Configuration" above.

k. Click **Save Changes**.

l. Enable the Service Bus, set Enabled switch to **Yes**.

7. To verify everything is working correctly, open your browser and point it to the ServiceBus worker service:

   - **On-Premises**: `https://yourinstance.privilegemanager.com/Tms/ServiceBus/WorkerService.svc`

   Wait for the page to respond.

Configuring Agents to Use the Service Bus

When setting the URL for Agent communication, Internet connected clients need to use the Service Bus URL created above.

Note: For new installations, the agents can be set up to communicate with the service bus during the initial installation process when the **TMSURL** and installation codes are provided, refer to Bundled Install.

Using regedit

1. Open the Registry Editor (**regedit**).
2. Navigate to **HKEY_LOCAL_MACHINE | SOFTWARE | Policies | Arellia | AMS**.
3. Right click **BaseUrl** and select **Modify**.
4. In the **Edit String** dialog box, change the **BaseURL** to your Privilege Manager (TMS) Address based on the **Azure Service Bus Queue** configuration, for example `https://[your company].servicebus.windows.net/`, which in our example is `https://testing.servicebus.windows.net/`
5. Close the Registry Editor.
6. Restart the Agent service.

Using PowerShell

To modify the TMS address via PowerShell, run this command as Administrator:

```
ERROR: Invalid Code Highlighting Language
```

The script will then ask you to type in the fully qualified domain name of the server, enter the **Azure Service Bus Queue URL**, for example `https://[your company].servicebus.windows.net/`, which in our example is `https://testing.servicebus.windows.net/`.

Setting up a Reverse Proxy

Many organizations as a best practice restrict their Privilege Manager web server from inbound and outbound internet traffic. However this can cause a functional issue as agents not connected to the corporate network would not be able to reach the server to receive policy updates or submit event feedback.

To resolve this functional issue while maintaining security Delinea supports agent connections through a Reverse Proxy which can live in the DMZ. The proxy will filter connection requests and only forward those from the agents allowing communication while significantly reducing the potential attack surface. Proxies can be configured using many different networking tools and in this document we will show how to do so with Windows Application Request Routing in IIS.

In this setup, only the endpoint agent needs to be accessible via HTTPS. It is important to note that the certificate being used for HTTPS communication should be the same certificate that is installed on your Privilege Manager web server.

> **Note:** Setting up a Proxy Server is specific to your organization's environment and configuration. Installation should be guided by your internal IT team.

Testing Agent URLs

To test registered agent URLs use the following, based on Privilege Manager version:

- /agent/agentregistration4.svc
- /agent/agentregistration3.svc
- /agent/agentregistration2.svc

For example using `https://PrivilegeManagerAppServerName.DomainName/TMS/Agent/agentregistration4.svc` at the agent agent point, should successfully return XML like the following:


```
▼<wsdl:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:wsx="http://schemas.xmlsoap.org/ws/2004/09/mex" xmlns:i0="http://tempuri.org/"
 xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsa10="http://www.w3.org/2005/08/addressing"
 xmlns:wsp="http://www.w3.org/ns/ws-policy" xmlns:wsap="http://schemas.xmlsoap.org/ws/2004/08/addressing/policy"
 xmlns:msc="http://schemas.microsoft.com/ws/2005/12/wsdl/contract" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
 xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:tns="http://arellia.com/services/Agent/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
 xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" name="Thycotic.Tms.Services.Agent.AgentRegistration4" targetNamespace="http://arellia.com/services/Agent/">
  <wsdl:import namespace="http://tempuri.org/" location="https://localhost/TMS/Agent/AgentRegistration4.svc?wsdl=wsdl1"/>
  <wsdl:types/>
 ▼<wsdl:service name="Thycotic.Tms.Services.Agent.AgentRegistration4">
  ▼<wsdl:port name="CustomBinding_IAgentRegistration2" binding="i0:CustomBinding_IAgentRegistration2">
     <soap12:address location="https://localhost/TMS/Agent/AgentRegistration4.svc"/>
   ▼<wsa10:EndpointReference>
      <wsa10:Address>https://localhost/TMS/Agent/AgentRegistration4.svc</wsa10:Address>
    </wsa10:EndpointReference>
  </wsdl:port>
 ▼<wsdl:port name="CustomBinding_IAgentRegistration21" binding="i0:CustomBinding_IAgentRegistration21">
     <soap12:address location="http://win-e6gkpm7j7tf/TMS/Agent/AgentRegistration4.svc"/>
   ▼<wsa10:EndpointReference>
    ▼<wsa10:Address>
       http://test-system/TMS/Agent/AgentRegistration4.svc
     </wsa10:Address>
    </wsa10:EndpointReference>
  </wsdl:port>
 </wsdl:service>
</wsdl:definitions>
```


Note: Make sure that the server acting as the reverse proxy trusts and matches the certificate that the Privilege Manager web server is using for its HTTPS binding. If the certificate is not trusted, the proxy will return a 500.21 Gateway error.

Agent Configuration

When you set up the Agent, make sure that the BaseURL has been set to the DMZ Server Address by following the steps in Setting the Privilege Manager Server Address.

Important: The Privilege Manager server is **not** able to push tasks to agents when the agents are not connected to the same network. However, the internet connected clients will automatically pull tasks from the server on a scheduled interval.

Removing Privilege Manager from a Combined Install

To remove the Privilege Manager instance from a combined install instance with Secret Server perform the following steps:

Remove the Privilege Manager to Secret Server Connection

1. Open SQL Management Studio and connect to the SQL Server that hosts the Secret Server database.
2. Expand Databases.
3. Right-click on the Secret Server database and choose **New Query**.

4. Copy the following query and paste into the *New Query* screen.

```
DELETE from [dbo].tbAppClient WHERE AppClientId = 1
UPDATE [dbo].tbConfiguration set TmsRootUrl = null
```

5. Click **Execute** to run the query.

Remove the TMS Site

1. Open IIS Manager and go to Application Pools.
2. Stop the TMS, TMSAgent and TMSWorker pools.
3. Expand Sites and find and expand the TMS site.
4. Right-click the following site applications and choose Remove:
   - TMS,
   - Agent,
   - ServiceBus,
   - Services,
   - Setup, and
   - Worker.
5. Navigate back to Application Pools and remove the TMS, TMSAgent and TMSWorker pools.

Remove the TMS Site Files and Registry Key

1. On the IIS Server, open File Explorer.
2. Find the TMS site folder (default: `c:\inetpub\wwwroot\TMS`)
3. Delete the TMS site folder.
4. Navigate to the Registry and remove the Registry key: `HKLM\Software\Thycotic\Tms`

Maintaining Your System

This topic is a collection of articles commoly-used procedures for maintaining different areas of the Privilege Manager product.

Instructions for performing specific actions and tasks can be found throughout the "Administration" on page 477 section, as applicable. Refer to "Infrastructure Scheduled Activities" on page 835 for a reference table of scheduled infrastructure activities.

Note: If you need to modify any items within Privilege Manager, duplicate the item and modify the duplicate instead of the built-in item so that an upgrade does not overwrite it.

The following topics are available:

- How to Purge Computers
- How to Purge the Action Items Table

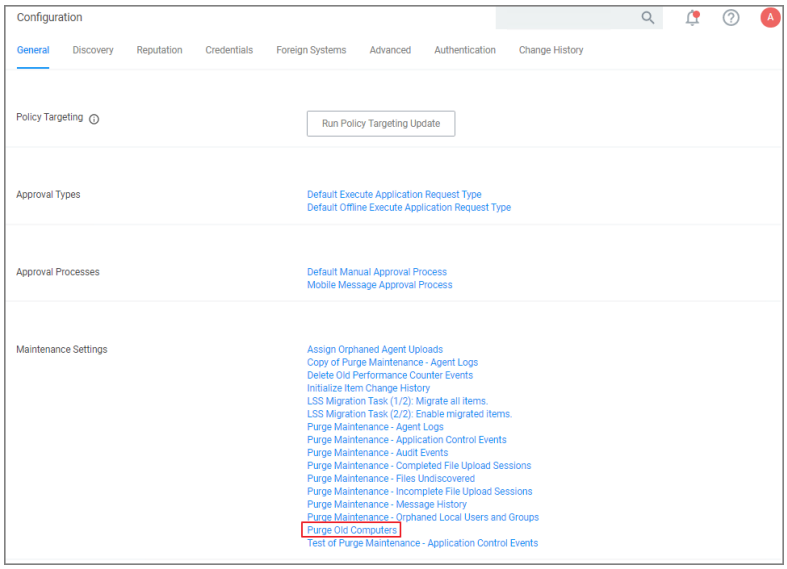
- Using the Remove Programs Utility
- Export Items
- Import Items
- Migrate Local Security Policies
- Remove Active Directory Domain
- Merge Duplicate Active Directory Domains

How to Purge Computers

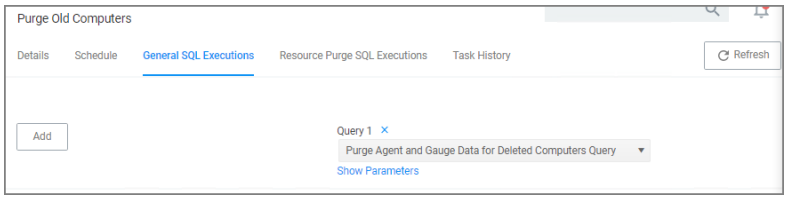
After using Privilege Manager for a certain amount of time, you may have computers that haven't communicated with the Privilege Manager server for an extended period of time. This can be done via the Purge Computers task, which can be found under Configuration on the General tab.

Note: If you need to modify any items within Privilege Manager, duplicate the item and modify the duplicate instead of the built-in item so that an upgrade does not overwrite it.

1. Navigate to **Admin | Configuration** and select the **General** tab.
2. Under the Maintenance Settings section click **Purge Old Computers**.



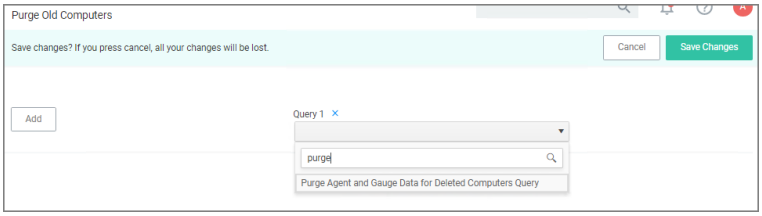
3. On the **Purge Old Computers** page select the **General SQL Executions** tab.
4. Verify that **Query 1** is set to **Purge Agent Gauge Data for Deleted Computers Query**.



If for whatever reason that specific query is not listed or if you need to add other queries,

a. Click **Add** to either replace the query currently listed or add this query.

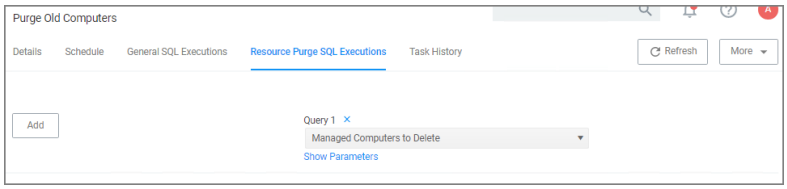
b. Start typing the query name *Purge Agent Gauge Data for Deleted Computers Query* and select the query from the results list.



c. Click **Save Changes**.

5. Select the Resource Purge SQL Executions tab.

6. Verify that **Query 1** is set to **Managed Computers to Delete**.



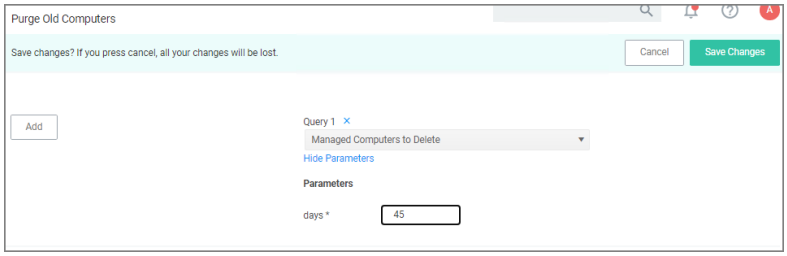
If that specific query is not listed,

a. Click **Add** to either replace the query currently listed or add this query.

b. Start typing the query name *Managed Computers to Delete* and select the query from the results list.

c. Click **Save Changes**

7. Click **Show Parameters**. The Days field indicates after how many days a system is considered to be an old computer and thus should be purged. The default value is 90 days. If you want a different value, enter a number to change the number of days.

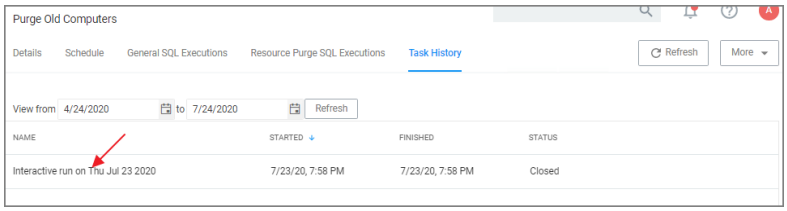


a. Click **Save Changes**.

8. Click **More | Run Task**.

9. On the **Task Name** modal, you may change the task name and click **Run Task**.

10. On the **Task History** tab you can view the status of the running task by selecting the task from the table grid.

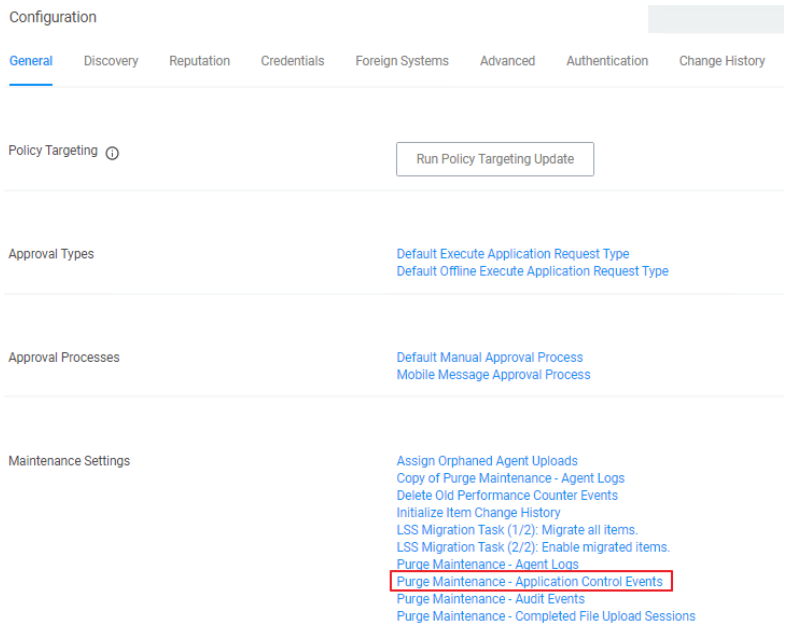


Purging Action Items Table

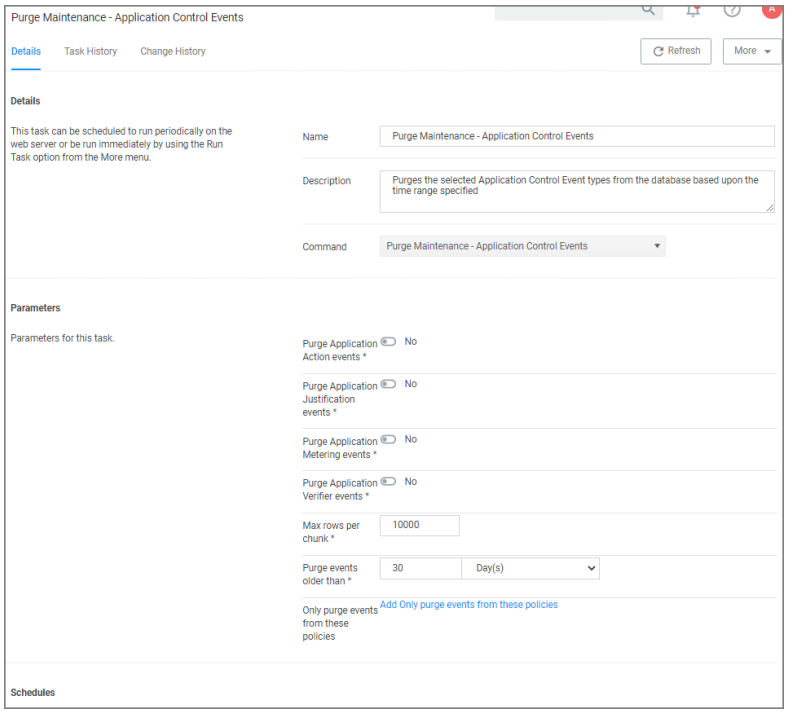
If the application action table frequently grows too large, you can use the steps below to create a scheduled event to purge old application action events.

Creating a Scheduled Event for Purging

1. Launch **Privilege Manager**.
2. Click **Admin | Configuration**.

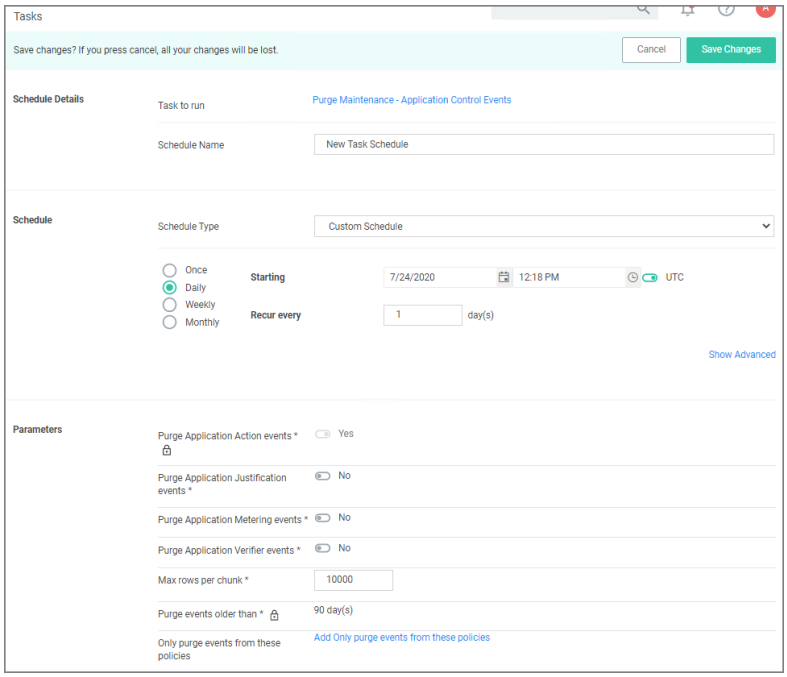


3. Click **Purge Maintenance – Application Control Events**.



4. Under **Parameters**,
   a. Set the **Purge Application Action events** switch to **Yes**.
   b. Under **Purge events older than** you may change the default of 30 days to another value.

      Note: You can also select the other events to purge as well.
5. Click **Save Changes**.
6. Under **Schedules** click **New Schedule**.



7. Enter in a **Schedule name** and the frequency you want the task to run. You can add other parameters here too. Parameters that were previously selected are locked at this point.
8. Click **Save Changes**.

Using the Remove Programs Utility

The Remove Programs Utility provides a solution to the following problem that Windows standard users are not able to remove applications from the control panel because of Windows checking for admin rights. This utility is available for deployment via Privilege Manager.

Customers can use this utility in any of the following ways:

- Allow users to uninstall any and all applications by using the utility.
- Make the utility show an approval request for each uninstaller that is launched.
- Make the utility show an approval prompt when it launches.

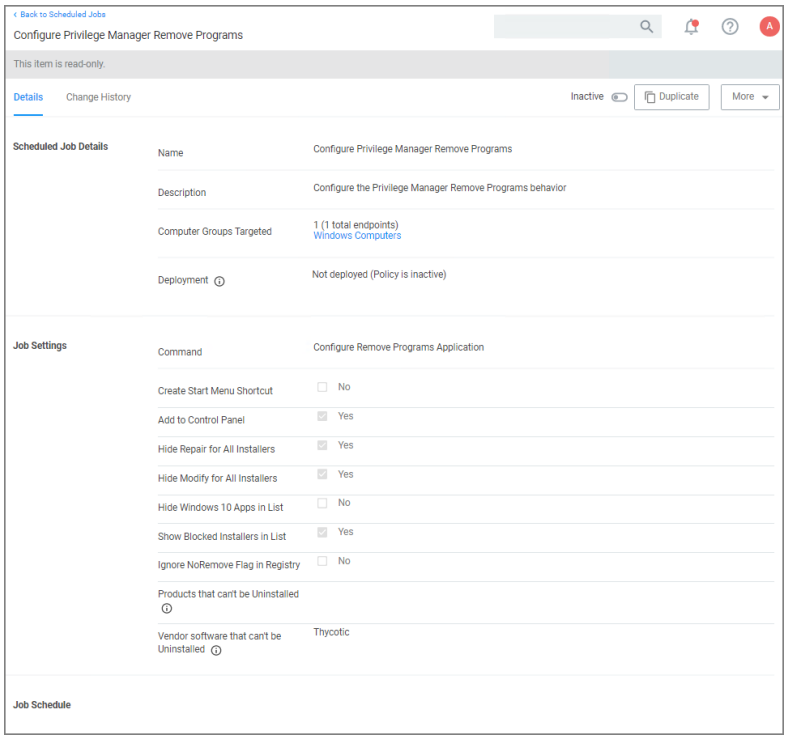
The utility will list all the same applications as the Remove Programs in the Control Panel, but it can also hide software that end users should not be able to uninstall (such as the Delinea agents).

With Privilege Manager version 10.7 Delinea introduced support for Windows 10 **Apps & Features** and the management of Windows Store apps via the **Remove Programs Helper**. Certain apps designed as a Windows 10 package are registered in **Apps & Features** but do not appear in the operating systems Add Remove Programs options. Privilege Manager locates those applications and provides management via the enhanced **Remove Programs Utility**.

> **Note:** The Remove Programs Utility does not work if your agents have FIPS enabled. You can either disable FIPS for your agents with AD Group Policy or target the uninstaller for a given application directly.

Configuring the Remove Programs Utility

1. Under your **Computer Group** select **Scheduled Jobs**.
2. Search for **Configure Privilege ManagerRemove Programs**.
3. Click on the policy link **Configure Privilege ManagerRemove Programs**.



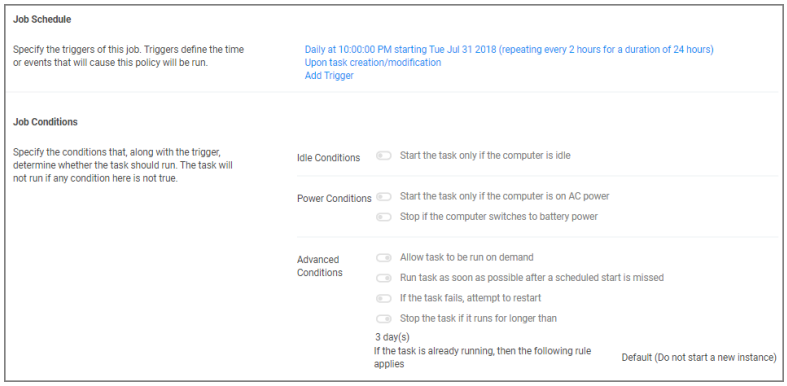
   If you need to customize the default policy, Delinea recommends to create a copy.

4. Click **Duplicate** and name your policy.
5. Click **Create**.
6. Under **Job Settings**, customize the access and functions of the utility. For example:
   - Choose whether a shortcut on the start menu or on the control panel should be created.
   - List products that you want to prevent being uninstalled. There are two options for this:
     - If the "Show Blocked Installers in List" option is unchecked, the products will be hidden.
     - If the "Show Blocked Installers in List" option is checked, the products will just be disabled from being uninstalled.

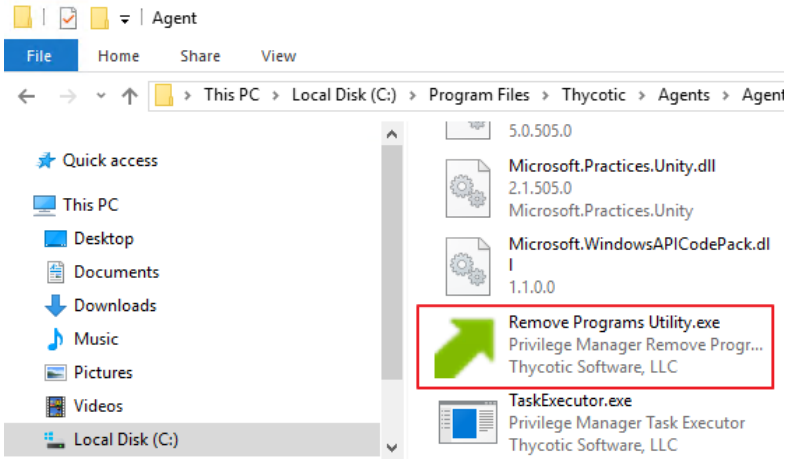
   If you selected "Create Start Menu Shortcut", the users will see Privilege ManagerRemove Programs on the Start Menu. If you selected "Add to Control Panel", the users will see Privilege ManagerRemove Programs in the Control Panel.

7. Under **Job Schedule**, customize the triggers, such as when to run the utility for inventory purposes. This determines how often you want the policy from the Task Scheduler on the endpoint to check to ensure the

settings match.

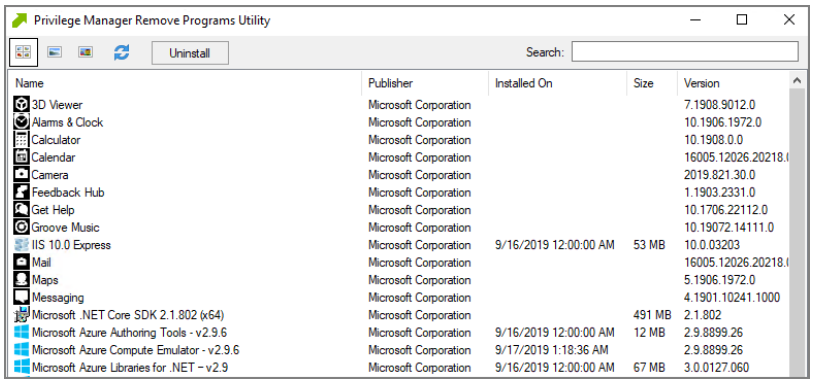


8. Under **Job Conditions**, customize additional conditions that impact running the task, e.g. allowing the utility to be used on demand.
9. Set the **Inactive** switch to **Active**.
10. Click **Save Changes**.
11. Next to **Deployment**, click the **i** icon and select the **Resource and Collection Targeting Update** task.



Using the Utility

The utility is straightforward to use. It's installed on endpoints as part of the Agents installation. Users can select the row containing the program that they want to uninstall and then select the uninstall button.



Using the Elevate Privilege ManagerRemove Programs Policy Children Policy (Sample)

Note: Starting with Privilege Manager agents version 11.0, the Remove Program Utility does not require elevation on endpoints.

Delinea recommends using the out-of-the-box **Elevate Privilege ManagerRemove Programs Policy Children Policy (Sample)** policy on endpoints that are configured to use the Remove Program Utility. This policy elevates the uninstallers only after an approval request has been granted.

You may also manually block non installers from running by importing the following block-non-installer-child-processes XML file.

Block Non-Installer Child Process XML

```
<items>
<ResourceContract xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schemas.microsoft.com/
xmlns:dc="http://schemas.datacontract.org/2004/07/System" xmlns:i="http://www.w3.org/2001/XMLSchema-i
    <adc:Attributes>NoModify NoReplication NoDelete</adc:Attributes>
    <adc:ItemId>4c628030-23ac-542c-b393-eab95dc471c0</adc:ItemId>
    <adc:Name>CN=Thycotic Software, OU=Development, O=Thycotic Software, L=Washington, S=District of
    <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
    <adc:Strings />
    <adc:Tags />
    <AdditionalResourceRoleIds />
    <ChildAssociations />
    <DataClassData>
        <adc:DataClassData>
            <adc:DataClassId>0577a870-283f-470f-8f9b-15fdab031e96</adc:DataClassId>
            <adc:DataClassType>InventorySingleRow</adc:DataClassType>
            <adc:DataSet>
                <dataset xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata" xmlns:sqltypes="http://schemas.microsoft.com/sqls
                    <DS_Digital_Certificate_Raw xmlns="http://schemas.arellia.com/resource/data/">
                        <Digital_Certificate_Raw c1="true">
```

```
                                <c0>
MIIE1zCCA7+gAwIBAgIQNAO/dhnl0ufyV5FDaH5srjANBgkqhkiG9w0BAQsFADBRMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMdGhhd
VowgY8xCzAJBgNVBAYTAlVTMR0wGwYDVQQIDBREaXN0cmljdCBvZiBDb2x1bWJpYTETMBEGA1UEBwwKV2FzaGluZ3RvbjEaMBgGA1
cNAQEBBQADggEPADCCAQoCggEBAMq/vBGY70gaoVrCNXQDl1L48mB0BNoKLh/TsE18EiLJFIingbw63euNbntQE1uEJyoWB6Nnp03
CoxepU+tTHKbtBTFJpwEZM1UvQlhGsxDdMGKpbUGto5hg+WWtBIbhmuRu6z9clam8A0x5NRxIViGmeo830sArHwrwVjRQ8ZLTYZtn
8lsKcM0RwWgKdvA9pVYwHQYDVR0OBBYEFPmhy6Dxk4ZgyUE8KeIwQfmFMS7BMCsGA1UdHwQkMCIwIKAeoByGGmh0dHA6Ly90by5zeW
wIBFhpodHRwczovL3d3dy50aGF3dGUuY29tL2NwczAvBggrBgEFBQcCAjAjDCFodHRwczovL3d3dy50aGF3dGUuY29tL3JlcG9zaX
9tL3RvLmNydDANBgkqhkiG9w0BAQsFAAOCAQEAKXO6r2nCFnGBOAd4i1PItY85/e3smYjYlQFcUPrwMBw3aGXUuFRHXeHXDXVo+ua
yaX8t5p0lD9z9CkFRBXu39qK7WFIZ1bKMynLr7NrMH6KU1O4ptsfEOOrN+HH/BzJdW+0+7a+0KArL7ItKv2VVrj/Lswp6QSASPxzD
                            </Digital_Certificate_Raw>
                        </DS_Digital_Certificate_Raw>
                    </dataset>
                </adc:DataSet>
            </adc:DataClassData>
            <adc:DataClassData>
                <adc:DataClassId>4d7c8bff-22c3-40f6-8f95-6410ebd4c1d9</adc:DataClassId>
                <adc:DataClassType>Inventory</adc:DataClassType>
                <adc:DataSet>
                    <dataset xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata" xmlns:sqltypes="http://schemas.microsoft.com/sqls
                        <DS_Hash xmlns="http://schemas.arellia.com/resource/data/">
                            <Hash c0="1a160ee1-61c1-41f2-8758-a7562e84b358" c1="Az0h0vQP6PGmeq23oy1NLdRVU
                            <Hash c0="3bc0e8a0-caa1-40e0-b705-c8d990c0babf" c1="TGKAMCOsVCyzk+q5XcRxwIOH3
                        </DS_Hash>
                    </dataset>
                </adc:DataSet>
            </adc:DataClassData>
            <adc:DataClassData>
                <adc:DataClassId>b5479b8c-425f-491c-b835-72c5d611fb1e</adc:DataClassId>
                <adc:DataClassType>InventorySingleRow</adc:DataClassType>
                <adc:DataSet>
                    <dataset xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata" xmlns:sqltypes="http://schemas.microsoft.com/sqls
                        <DS_Digital_Certificate_Details xmlns="http://schemas.arellia.com/resource/data/"
                            <Digital_Certificate_Details c2="rmx+aEORV/Ln0uUZdr8DNA==" c3="c36bc09f-1d7e-
                                <c0>CN=Thycotic Software, OU=Development, O=Thycotic Software, L=Washingt
                                <c1>CN=thawte SHA256 Code Signing CA - G2, O="thawte, Inc.", C=US</c1>
                                <c4>
MIIBCgKCAQEAyr+8EZjvSBqhWsI1dAOXUvjyYHQE2gouH9OwTXwSIskUiKeBvDrd641ue1ATW4QnKhYHo2enTe8CG8q6d9WfjYnlSu
UmnARkzVS9CWEazEN0wYqltQa2jmGD5Za0EhuGa5G7rP1yVqbwDTHk1HEhWIaZ6jzfSwCsfCvBWNFDxktNhm2eLryczmVtuFt0Dvj
                            </Digital_Certificate_Details>
                        </DS_Digital_Certificate_Details>
                    </dataset>
                </adc:DataSet>
            </adc:DataClassData>
        </DataClassData>
        <OwnsItemIds />
        <ResourceTypeId>c76fc2a7-85db-4ecb-a055-8cd0d5fc91fd</ResourceTypeId>
    </ResourceContract>
    <ResourceContract xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schemas.microsoft.com/
    xmlns:dc="http://schemas.datacontract.org/2004/07/System" xmlns:i="http://www.w3.org/2001/XMLSchema-i
        <adc:Attributes>NoModify NoReplication NoDelete</adc:Attributes>
        <adc:ItemId>7777b584-ed00-502b-a0b9-a7d05b7e7f3d</adc:ItemId>
```

```
    <adc:Name>CN="Thycotic Software, LLC", O="Thycotic Software, LLC", L=Washington, S=District of Co
    <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
    <adc:Strings />
    <adc:Tags />
    <AdditionalResourceRoleIds />
    <ChildAssociations />
    <DataClassData>
        <adc:DataClassData>
            <adc:DataClassId>0577a870-283f-470f-8f9b-15fdab031e96</adc:DataClassId>
            <adc:DataClassType>InventorySingleRow</adc:DataClassType>
            <adc:DataSet>
                <dataset xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata" xmlns:sqltypes="http://schemas.microsoft.com/sqls
                    <DS_Digital_Certificate_Raw xmlns="http://schemas.arellia.com/resource/data/">
                        <Digital_Certificate_Raw c1="true">
                            <c0>
MIIGRzCCBS+gAwIBAgIQCtD5u/YJCUkTGHQ/ld9sZzANBgkqhkiG9w0BAQsFADByMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlna
ENBMB4XDTIwMDcyNzAwMDAwMFoXDTIzMDgwMTEyMDAwMFowgYMxCzAJBgNVBAYTAlVTMR0wGwYDVQQIExREaXN0cmljdCBvZiBDb2
dhcmUsIExMQzCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALn6VfpuO1u4mGSnn2fRdpI+SrV/y0Euswobgbjrt6J8Czz
ZiChe8Xd0IMcD215f2IAhWNRir840wyOb1Uz7yUtSk2e4yeGE/7xol4BMStpBkwU4kn3KWGnwh5LYEPEtJeiye/6o1maFWwnrCpyk
Xfgy3XQjMrIMQcwA3MyXI1iAZwMRukmtDIVIyS1I1mazw5ZQ1U8p+i6YTxkpQTrbf/75C8xxpzAuMLzqWZRjlYPKRZfHeQu1xrcBU
XeuJAESn6QfzqTN0K3HSi0/A4fAEol1MNhN0rl6sV1ZFv98+dHzo1T3xKt9S9JgTFUyvMunS/+TnFmGhV1UQMU2Y9D9iWzXLnG/Ag
H/BAQDAgeAMBMGA1UdJQQMMAoGCCsGAQUFBwMDMHcGA1UdHwRwMG4wNaAzoDGGL2h0dHA6Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9zaGE
DMDcGCWCGSAGG/WwDATAqMCgGCCsGAQUFBwIBFhxodHRwczovL3d3dy5kaWdpY2VydC5jb20vQ1BTMAgGBmeBDAEEATCBhAYIKwYB
LmNvbS9EaWdpQ2VydFNIQTJBc3N1cmVkSURDb2RlU2lnbmluZ0NBLmNydDAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBCwUAA4IBA
2JYUKSRVJ6YrJOjJnIHhN5rsok7pZlLkPcEiNT3/Zxk2SNWYK6mMgQRGzVMeIXdOWGJeHpXvj89Xians7N46U1Uw4DQtUXuCgoiw
eCEg0Ld5bd7jSz0iNY</c0>
                        </Digital_Certificate_Raw>
                    </DS_Digital_Certificate_Raw>
                </dataset>
            </adc:DataSet>
        </adc:DataClassData>
        <adc:DataClassData>
            <adc:DataClassId>4d7c8bff-22c3-40f6-8f95-6410ebd4c1d9</adc:DataClassId>
            <adc:DataClassType>Inventory</adc:DataClassType>
            <adc:DataSet>
                <dataset xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata" xmlns:sqltypes="http://schemas.microsoft.com/sqls
                    <DS_Hash xmlns="http://schemas.arellia.com/resource/data/">
                        <Hash c0="1a160ee1-61c1-41f2-8758-a7562e84b358" c1="E0ez9lcH+o3PzskLruwYLKsnv
                        <Hash c0="3bc0e8a0-caa1-40e0-b705-c8d990c0babf" c1="d3e1hO0AACsguafQW35/PS4/0
                    </DS_Hash>
                </dataset>
            </adc:DataSet>
        </adc:DataClassData>
        <adc:DataClassData>
            <adc:DataClassId>b5479b8c-425f-491c-b835-72c5d611fb1e</adc:DataClassId>
            <adc:DataClassType>InventorySingleRow</adc:DataClassType>
            <adc:DataSet>
                <dataset xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata" xmlns:sqltypes="http://schemas.microsoft.com/sqls
                    <DS_Digital_Certificate_Details xmlns="http://schemas.arellia.com/resource/data/"
                        <Digital_Certificate_Details c2="Z2zflT9OGBNJCQn2u/nQCg==" c3="c36bc09f-1d7e-
```

```
                                <c0>CN="Thycotic Software, LLC", O="Thycotic Software, LLC", L=Washington
                                <c1>CN=DigiCert SHA2 Assured ID Code Signing CA, OU=www.digicert.com, O=D
                                <c4>
MIICCgKCAgEAufpV+m47W7iYZKefZ9F2kj5KtX/LQS6zChuBsmu3onwLPM3afjlXyBVOCl4a322ZmdBmmqPwSOckp8e/jSXafcrrI
7jJ4YT/vGiXgExK2kGTBTiSfcpYafCHktgQ8S0l6LJ7/qjWZoVbCesKnKTNFK+AjBbsvRXTe6ZvdrmKU4+2MdEbVOzawdUSByWPiM
NbllDVTyn6LphPGSlBOtt//vkLzHGnMC4wvOpZlGOVg8pFl8d5C7XGtwFQiAxhGWMb+mVSMsXTDS0aQZG8FdIZ7ratC2XcIatEjSK
W/3z50fOjVPfEq31LOmBMVTK8y6dL/5OcWYaFXVRAxTZj0P2JbNcucb8CAwEAAQ==</c4>
                        </Digital_Certificate_Details>
                    </DS_Digital_Certificate_Details>
                </dataset>
            </adc:DataSet>
        </adc:DataClassData>
    </DataClassData>
    <OwnsItemIds />
    <ResourceTypeId>c76fc2a7-85db-4ecb-a055-8cd0d5fc91fd</ResourceTypeId>
</ResourceContract>
<DigitalCertFilterContract xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schemas.micros
xmlns:dc="http://schemas.datacontract.org/2004/07/System" xmlns:d1p4="http://schemas.arellia.com/dc/C
instance" xmlns="http://schemas.arellia.com/dc/FileInventory/Filters/">
    <adc:Attributes>NoModify NoReplication NoDelete</adc:Attributes>
    <adc:FolderId>bd1b4d12-8dfc-4fcf-a6ea-fe09159ff055</adc:FolderId>
    <adc:ItemId>d1ca1c62-43de-4140-b8c5-85471c106a0f</adc:ItemId>
    <adc:Name>Signed by Thycotic Certificate Filter</adc:Name>
    <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
    <adc:Strings />
    <adc:Tags>
        <arr:string>pm.platform.windows</arr:string>
    </adc:Tags>
    <ChildAssociations />
    <DigitalCertIds>
        <arr:guid>7777b584-ed00-502b-a0b9-a7d05b7e7f3d</arr:guid>
        <arr:guid>4c628030-23ac-542c-b393-eab95dc471c0</arr:guid>
    </DigitalCertIds>
    <OwnsItemIds />
    <SubjectName i:nil="true" />
</DigitalCertFilterContract>
<Win32ExeFilterContract xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schemas.microsof
xmlns:dc="http://schemas.datacontract.org/2004/07/System" xmlns:d1p4="http://schemas.arellia.com/dc/C
instance" xmlns="http://schemas.arellia.com/dc/FileInventory/Filters/">
    <adc:Attributes>NoModify NoReplication NoDelete</adc:Attributes>
    <adc:FolderId>bd1b4d12-8dfc-4fcf-a6ea-fe09159ff055</adc:FolderId>
    <adc:ItemId>eca86824-14f4-4301-8667-cfa316a00a39</adc:ItemId>
    <adc:Name>Privilege Manager 'Remove Programs Utility.exe' Executable Filter</adc:Name>
    <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
    <adc:Strings />
    <adc:Tags>
        <arr:string>pm.platform.windows</arr:string>
    </adc:Tags>
    <CompanyName />
    <DriveTypes>0</DriveTypes>
    <ExeProductName>Privilege Manager</ExeProductName>
    <FileName />
    <FilePath />
```

```
    <FilePathSubdir>false</FilePathSubdir>
    <FileVersion />
    <InternalName />
    <LegalCopyright i:nil="true" />
    <LocalDiscoveryInterval>0</LocalDiscoveryInterval>
    <OriginalFileName>Remove Programs Utility.exe</OriginalFileName>
    <ProductVersion />
    <UseLocalDiscoveryInterval>false</UseLocalDiscoveryInterval>
</Win32ExeFilterContract>
<FileSpecificationFilterContract xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schemas
xmlns:dc="http://schemas.datacontract.org/2004/07/System" xmlns:d1p4="http://schemas.arellia.com/dc/C
instance" xmlns="http://schemas.arellia.com/dc/FileInventory/Filters/">
    <adc:Attributes>NoModify NoReplication NoDelete</adc:Attributes>
    <adc:FolderId>bd1b4d12-8dfc-4fcf-a6ea-fe09159ff055</adc:FolderId>
    <adc:ItemId>f44edf77-0fd5-4d30-b0ad-ad1a5da7351c</adc:ItemId>
    <adc:Name>Privilege Manager 'Remove Programs Utility.exe' File Specification Filter</adc:Name>
    <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
    <adc:Strings />
    <adc:Tags>
        <arr:string>pm.platform.windows</arr:string>
    </adc:Tags>
    <ChildAssociations>
        <arr:anyType i:type="adc:ItemAssociations">
            <adc:AssociationTypeId>efb89861-0aed-5592-be87-6c8992773a87</adc:AssociationTypeId>
            <adc:AssociatedItemIds />
        </arr:anyType>
        <arr:anyType i:type="adc:ItemAssociations">
            <adc:AssociationTypeId>c01776a1-dffd-5842-94ad-aedbafc19515</adc:AssociationTypeId>
            <adc:AssociatedItemIds />
        </arr:anyType>
    </ChildAssociations>
    <DriveTypes>0</DriveTypes>
    <ExcludeFilterIds />
    <FilePath i:nil="true" />
    <FileSpec i:nil="true" />
    <IncludeFilterIds />
    <IncludeHidden>false</IncludeHidden>
    <IncludeReparse>false</IncludeReparse>
    <IncludeSubdirectories>false</IncludeSubdirectories>
    <IncludeSystem>false</IncludeSystem>
    <IncludeSystemReparse>false</IncludeSystemReparse>
    <ManditoryFilterIds>
        <arr:guid>d1ca1c62-43de-4140-b8c5-85471c106a0f</arr:guid>
        <arr:guid>eca86824-14f4-4301-8667-cfa316a00a39</arr:guid>
    </ManditoryFilterIds>
    <OwnsItemIds />
</FileSpecificationFilterContract>
<ParentProcesssFilterContract xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schemas.mi
xmlns:dc="http://schemas.datacontract.org/2004/07/System" xmlns:d1p4="http://schemas.arellia.com/dc/C
instance" xmlns="http://schemas.arellia.com/dc/ApplicationControl/ApplicationFilter/">
    <adc:FolderId>bd1b4d12-8dfc-4fcf-a6ea-fe09159ff055</adc:FolderId>
    <adc:ItemId>a6e3701b-e6f2-47af-ab0f-6bfcb5c0c742</adc:ItemId>
    <adc:Name>Privilege Manager 'Remove Programs Utility.exe' Parent Process Filter</adc:Name>
```

```
    <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
    <adc:Strings />
    <adc:Tags>
        <arr:string>pm.platform.windows</arr:string>
    </adc:Tags>
    <ChildAssociations />
    <ExcludeFilterIds />
    <IncludeFilterIds>
        <arr:guid>f44edf77-0fd5-4d30-b0ad-ad1a5da7351c</arr:guid>
    </IncludeFilterIds>
    <ManditoryFilterIds />
    <OwnsItemIds />
</ParentProcesssFilterContract>
<Win32ExeFilterContract xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schemas.microsof
xmlns:dc="http://schemas.datacontract.org/2004/07/System" xmlns:d1p4="http://schemas.arellia.com/dc/C
instance" xmlns="http://schemas.arellia.com/dc/FileInventory/Filters/">
    <adc:Attributes>NoReplication System</adc:Attributes>
    <adc:Description>Filter used to identify the Windows Console Window</adc:Description>
    <adc:FolderId>f3355929-f372-43bd-83b0-3754f92f0e2e</adc:FolderId>
    <adc:ItemId>cbbf212a-b08b-4211-97ae-7b7db252ac3e</adc:ItemId>
    <adc:Name>Console Window Host (conhost.exe)</adc:Name>
    <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
    <adc:Strings />
    <adc:Tags />
    <CompanyName />
    <DriveTypes>0</DriveTypes>
    <ExeProductName />
    <FileName>conhost.exe</FileName>
    <FilePath>%SYSTEMROOT%\System32</FilePath>
    <FilePathSubdir>false</FilePathSubdir>
    <FileVersion />
    <InternalName />
    <LegalCopyright i:nil="true" />
    <LocalDiscoveryInterval>0</LocalDiscoveryInterval>
    <OriginalFileName />
    <ProductVersion />
    <UseLocalDiscoveryInterval>false</UseLocalDiscoveryInterval>
</Win32ExeFilterContract>
<ApplicationControlPolicyContract xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schema
xmlns:dc="http://schemas.datacontract.org/2004/07/System" xmlns:i="http://www.w3.org/2001/XMLSchema-i
    <adc:Attributes>NoReplication</adc:Attributes>
    <adc:Description>This policy blocks non-installers launched from the Privilege Manager Remove Pro
    <adc:FolderId>d60954d0-4bd3-4e2d-92cc-a00606d0e651</adc:FolderId>
    <adc:ItemId>429b2a7c-b95a-4926-bb29-51262b2a2f04</adc:ItemId>
    <adc:Name>Block Non-Installers from Privilege Manager Remove Programs Utility Policy</adc:Name>
    <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
    <adc:Strings />
    <adc:Tags>
        <arr:string>pm.platform.windows</arr:string>
        <arr:string>pm.policyType:block</arr:string>
    </adc:Tags>
    <adc:ApplyToResourcesSettings xmlns:d2p1="http://schemas.arellia.com/dc/Resource/">
        <d2p1:AllowedTargetRoleTypeId>493435f7-3b17-4c4c-b07f-c23e7ab7781f</d2p1:AllowedTargetRoleTyp
```

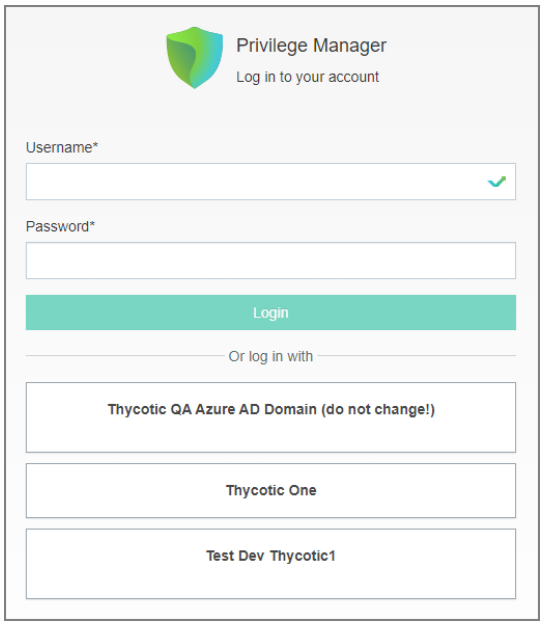
```
        <d2p1:RequiresScopingSecurity>false</d2p1:RequiresScopingSecurity>
        <d2p1:RestrictionCollectionId>00000000-0000-0000-0000-000000000000</d2p1:RestrictionCollectio
        <d2p1:ScopingSecurityOperationId>00000000-0000-0000-0000-000000000000</d2p1:ScopingSecurityOp
    </adc:ApplyToResourcesSettings>
    <adc:DefaultResourceTargetIds>
        <arr:guid>eb5326c2-dfbe-4399-8c53-d980a673fd95</arr:guid>
    </adc:DefaultResourceTargetIds>
    <adc:Enabled>false</adc:Enabled>
    <ApplicationActionIds>
        <arr:guid>01b913fe-b098-4ec9-99fe-ec93782da543</arr:guid>
    </ApplicationActionIds>
    <AppliesToAllProcesses>false</AppliesToAllProcesses>
    <ChildApplicationActionIds />
    <ChildAssociations />
    <EndsProcessing>true</EndsProcessing>
    <EndsProcessingChild>true</EndsProcessingChild>
    <ManditoryFilterIds>
        <arr:guid>a6e3701b-e6f2-47af-ab0f-6bfcb5c0c742</arr:guid>
    </ManditoryFilterIds>
    <NegativeFileFilterIds />
    <OwnsItemIds />
    <PositiveFileFilterIds>
        <arr:guid>71ca8447-6c03-4c6b-94cc-2e4ef3066c0b</arr:guid>
        <arr:guid>cbbf212a-b08b-4211-97ae-7b7db252ac3e</arr:guid>
        <arr:guid>ab4c795a-93e1-4c29-a67e-b6fcb5238ed1</arr:guid>
    </PositiveFileFilterIds>
    <Priority>3</Priority>
    <SendActionEvent>true</SendActionEvent>
    <SkipDuringSystemStartup>false</SkipDuringSystemStartup>
    <Stage2Processing>false</Stage2Processing>
</ApplicationControlPolicyContract>
</items>
```


Login and Logout Scenarios

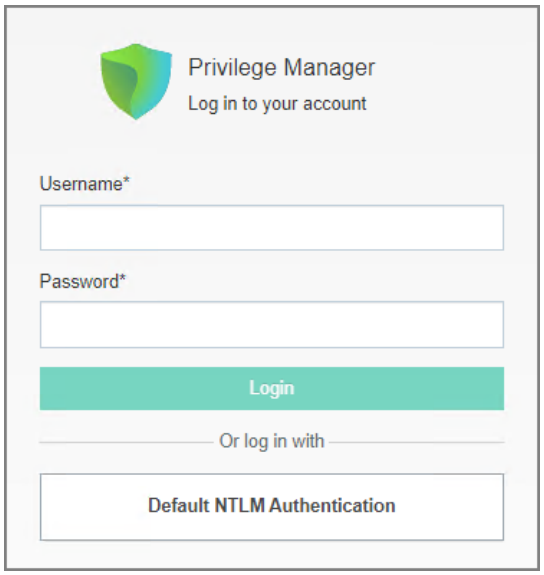
Based on authentication provider configured and used, the login and logout prompts and scenarios differ.

Login Options

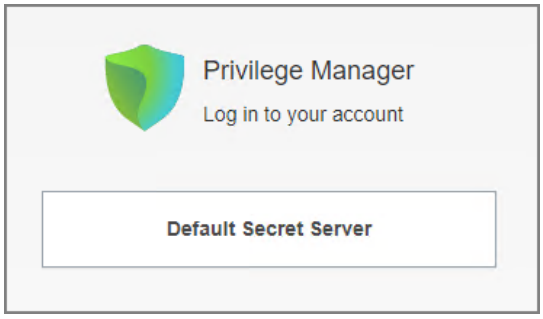
Sample images with various login options set up.



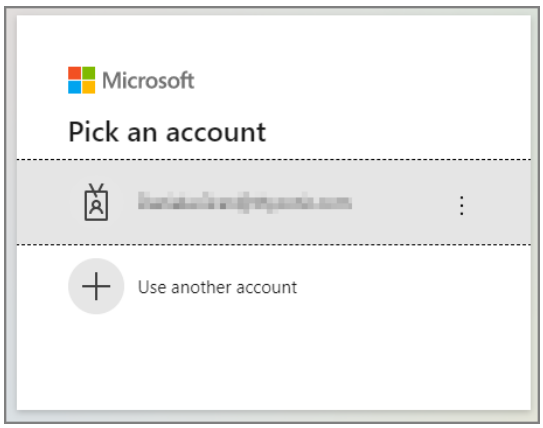
Basic login (Standard Out-Of-Box)



Basic login (Secret Server)



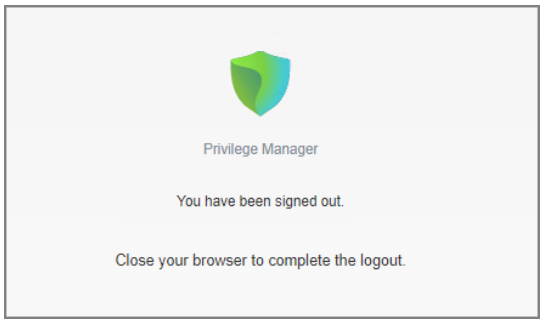
Azure AD



Logout Scenarios

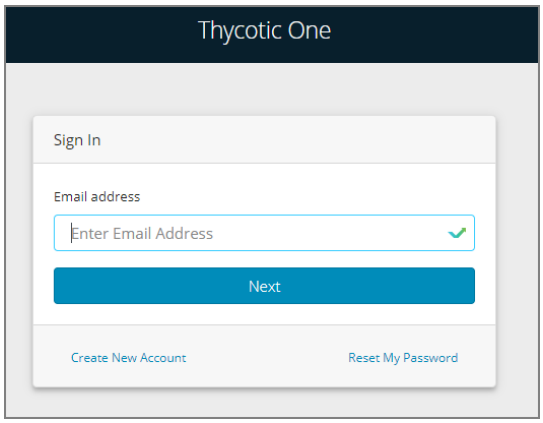
Basic with NTLM

After the logout completes, and the tokens are cleared, the user is presented with a prompt to close the browser.



Azure AD

After the logout completes, and the user tokens are cleared, the user is redirected to the Thycotic One login modal.



Platforms

Although Privilege Manager provided feature parity across all supported operating system, there are best practices and some functional areas that differ and are detailed in this section's topics.

For platform specific details, refer to:

- macOS
- Windows

Privilege Manager on macOS

On macOS endpoints, best practices around preference panes and user file and folder access varies from how these areas are managed on other operating system endpoints.

Changes introduced with Catalina and completed with Big Sur required a new approach from Privilege Manager.

The following topics provide details on platform specific information:

- "macOS Extensions" on the next page
- "macOS Secure Token" on page 152
- "Getting Started with macOS" below
- "macOS Gatekeeper" on page 155

Getting Started with macOS

Refer to the following topics for prerequisites that allow for an environment-wide macOS deployment:

- System Extensions: "Using MDM Profiles for your Agent" on page 194
- Allow Notifications:"Best Practices: Manage Privilege Manager Notifications on macOS" on page 18
- Approvals: "Application Approval Request Message Action" on page 338
- Agent Installation Overview: "Installing macOS Agents" on page 63

- Unattended Agent Install: "Installing macOS Agents" on page 63
- Deployment via Jamf: "Jamf Integration" on page 634

Best Practices

This best practices section pertains to all macOS versions from Big Sur to (and including) Ventura.

Delinea supports elevation without having to enter admin credentials for these preference panes:

- Date & Time
- Energy Saver
- Network
- Lock Screen

Other preference panes should not be used in elevation policies based on the nature of their function within the system. They can be elevated, but for certain actions, admin credentials may still be required. Changing those preference panes' settings should really be done by administrators only and not standard users, as designed by Apple.

All macOS preference panes can be used in deny policies.

This section contains macOS specific user interface topics.

- "Getting Started with macOS" on the previous page
- "Privilege Manager on macOS" on the previous page
- "Printer Installs" on page 171
- "Date & Time Preference Pane" on page 160
- "Energy Saver Preference Pane" on page 163
- "Battery Preference Pane" on page 158
- "Network Preference Pane" on page 166
- "Lock Screen Preference Pane" on page 171

macOS Extensions

Introduced with Catalina and fully implemented with Big Sur, Apple announced the deprecation of kernel extensions and replaced them with system extensions. The macOS agent implements a system extension and it is the core of policy enforcement.

You can read more about system extensions on Apple's website.

Legacy Kernel Extensions (KEXT)

The legacy and now deprecated flavor of the macOS agent is composed of several components and at the core of it are the KEXT and ThycoticACSvc daemon. They work together to enforce policy.

Effect on Privilege Manager Customers by Apple Deprecating Kernel Extensions in macOS

In 2019, Apple announced the deprecation of kernel extensions (KEXTS) in a future OS upgrade and that System Extensions should be used instead. Beginning in macOS 10.15.4, the use of kernel extensions will trigger a notification that software using this type of extension includes a deprecated API and an alternative should be provided by the vendor.

How Does This Affect Privilege Manager?

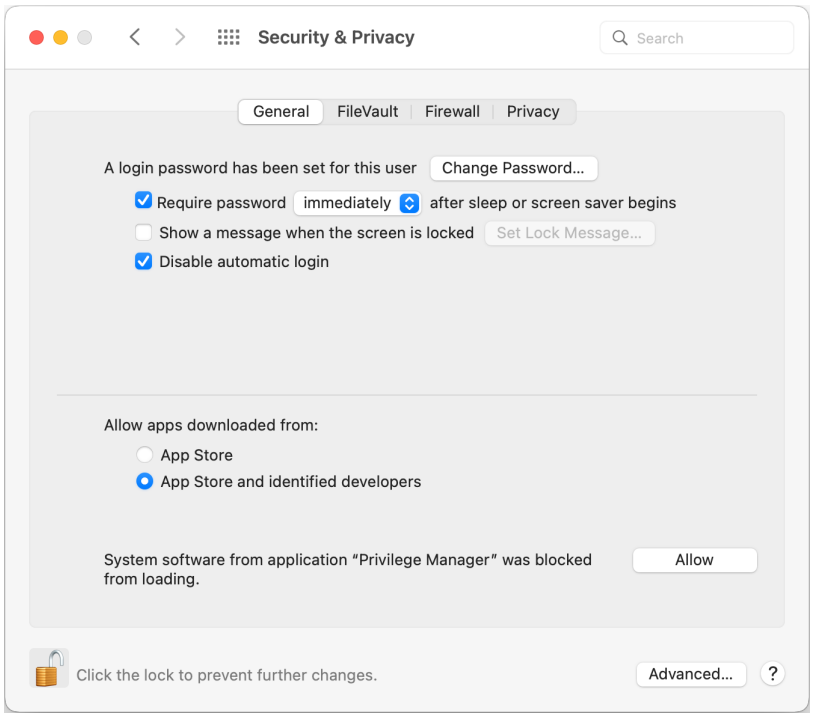
All new macOS agent functionality is implemented with a system extension for policy enforcement. The KEXT-based macOS agent will continue to function on supported versions of macOS up to and including Catalina. However, no new feature functionality will be made available. To take advantage of new features, you should upgrade to the latest version of Privilege Manager that supports your endpoints.

Using a Privacy Preference Policy Control Configuration Profile Payload

Privacy Preference Policy Control (PPPC) configuration profile payload allow for enterprises to manage and ease, through Mobile Device Management (MDM), the installation process of products that leverage KEXTs and SYSEXs for their end-users. When properly configured, this eliminates the need for the user to deal with all of the dialogs below.

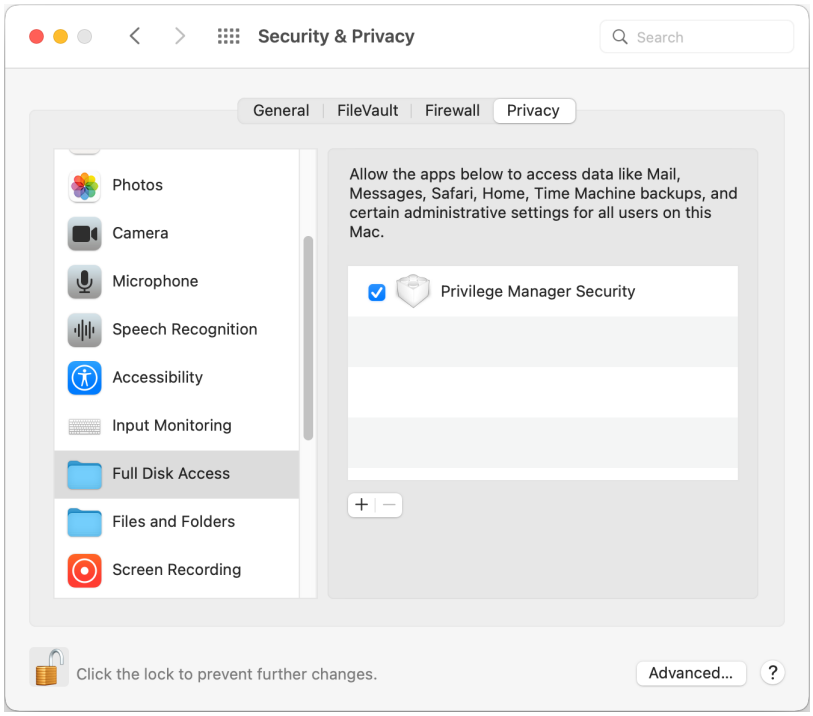
Delinea can provide the necessary configuration payloads that can be loaded into or leveraged with your MDM solution.

Allow System Extension

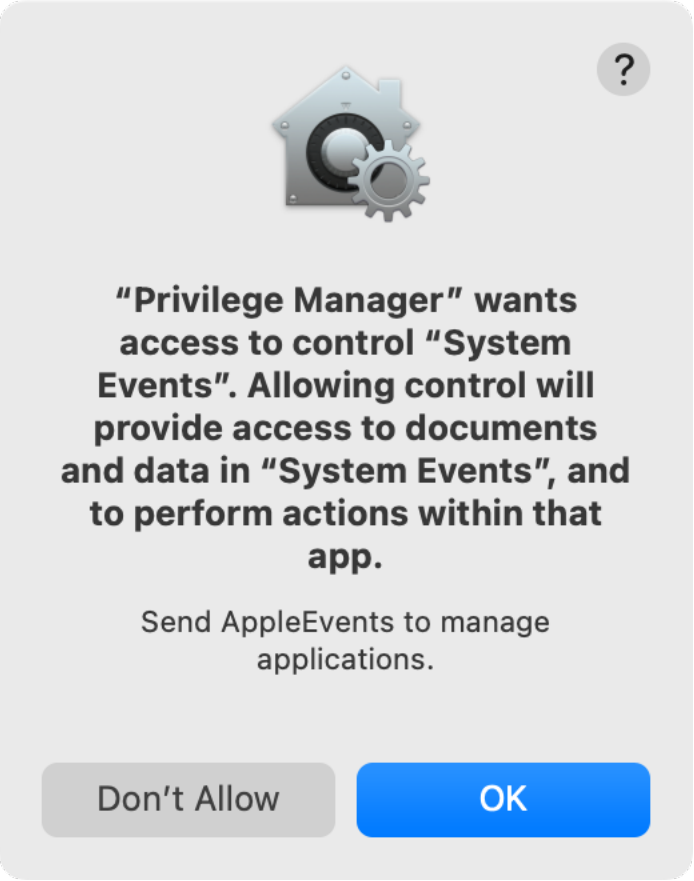


If you're not delivering a PPPC configuration profile via MDM to manage this, users will need to give Privilege Manager Security Full Disk Access.

Full Disk Access

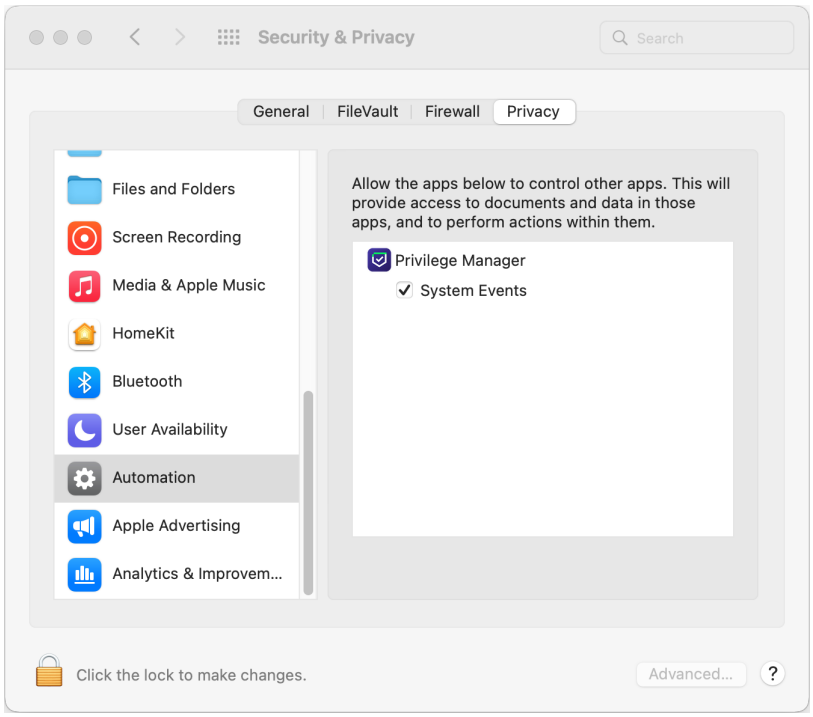


Allow System Events

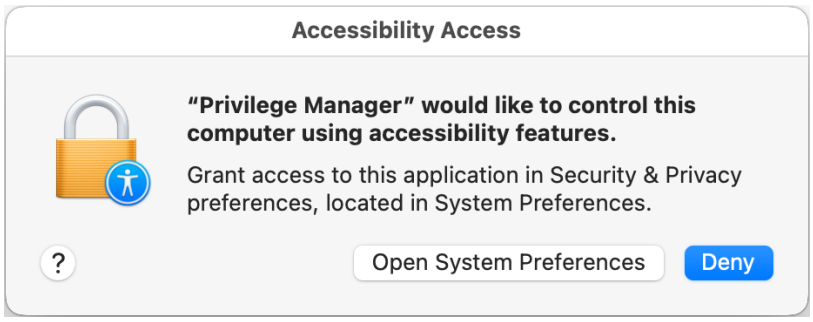


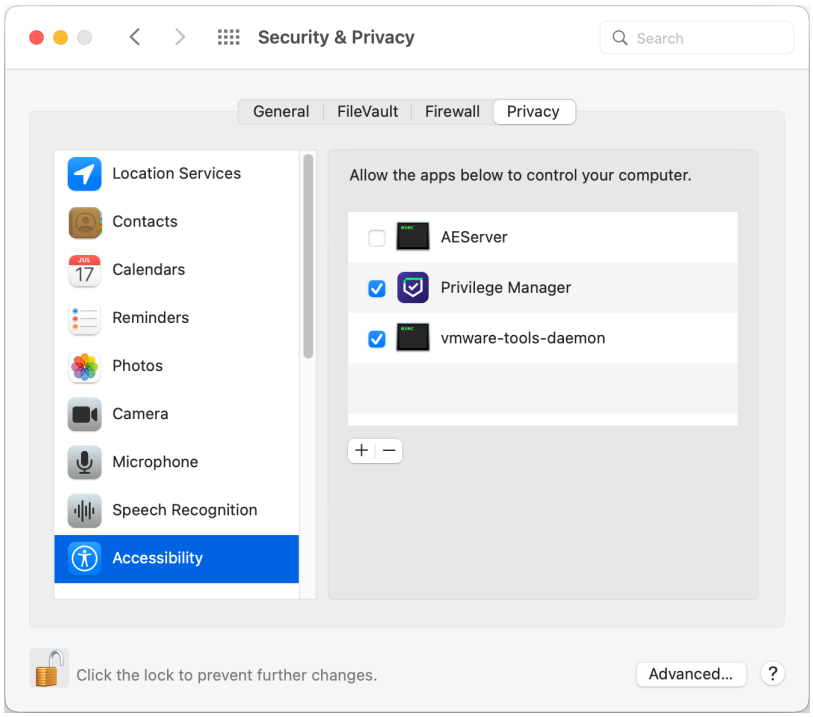
Clicking **OK** enables Privilege Manager to send AppleEvents to manage application windows. This setting can be found in **System Preferences** | **Security & Privacy** | **Privacy** | **Automation**.

Platforms



Accessibility





macOS Secure Token

Secure Token is a macOS High Sierra or later account attribute, that is required to be added to a user account before that account can be enabled for FileVault on an encrypted Apple File System (APFS) volume. To help make sure that at least one account has a Secure Token attribute associated with it, a Secure Token attribute is automatically added to the first account to log into the OS login window on a particular Mac. Once an account has a Secure Token associated with it, it can create other accounts which will in turn automatically be granted their own Secure Token.

In order for Privilege Manager to support Secure Token during account creation and for password management, a local account with Secure Token enabled must be created on each macOS workstation. The credentials for this account must be set as the Secure Token Management Credential.

When the Secure Token Management Credential is configured in the macOS agent configuration, Privilege Manager will use this credential to create a local account on each macOS workstation. The resulting managed local account will be used during account provisioning and password management to ensure that managed accounts are Secure Token enabled.

If the Secure Token Management Credential is removed in the macOS Agent Configuration, the agent will use the non-Secure Token enabled method of password management and any new users created/managed will not be Secure Token enabled. Any existing users that are Secure Token enabled will fail to have their password managed because without a Secure Token Management Credential macOS will not allow the agent to manage the password of a Secure Token enabled user.

> **Note:** The agent will ignore attempts to manage the service account. This includes provisioning and password management of the service account via LSS. You should not modify the service account, this includes changing its local password. Doing so may invalidate its configuration and cause the agent to fail password management.

Using Multiple Secure Tokens

To Implement multiple Secure Tokens across your macOS estate, you will be required to create a new agent configuration profile within your designated Computer Group.

Using an agent configuration that was created or duplicated using version 11.4.3 or earlier will continue to update the secure token in all agent configurations.

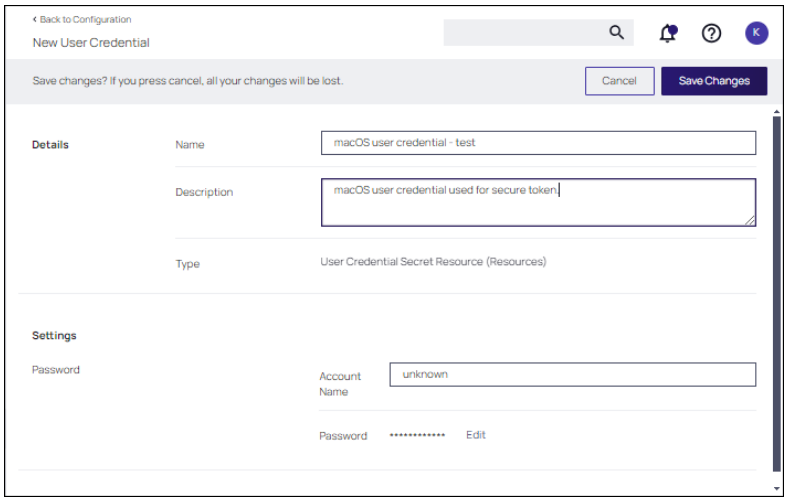
Considerations

- Agents should only belong to a single Computer Group with an active agent configuration.
- The primary agent configuration will need to be disabled, otherwise other configurations will be ignored.
- If an agent is added to more than one Computers Group with an active configuration, the agent may not follow the expected configuration.

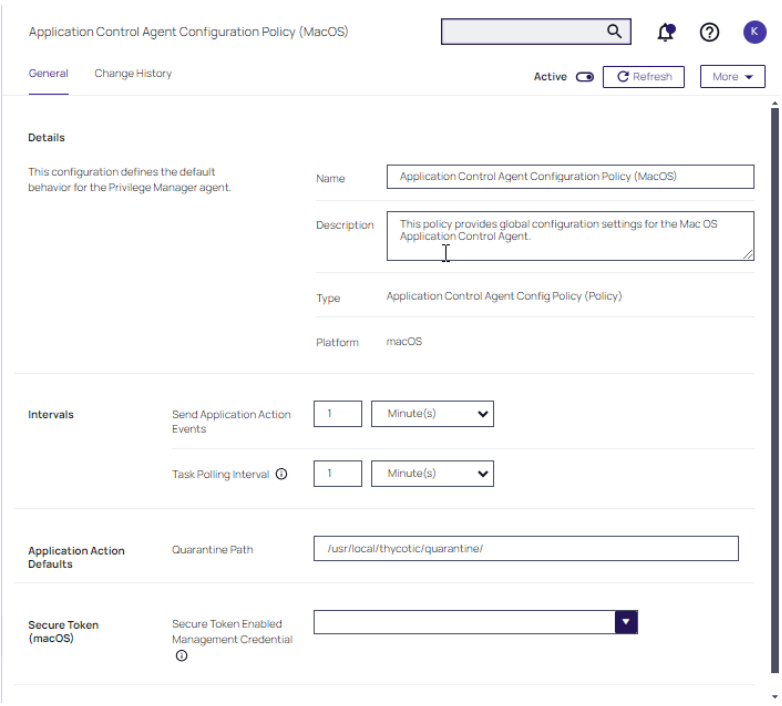
Agent Configuration

To use the Secure Token with macOS Agents, the user credential needs to be established and linked to the macOS agent configuration.

1. Navigate to **Admin | Configuration**, select the **Credentials** tab.
2. Click **Create**.



3. Under **Details** enter a **Name** and **Description**.
4. Under **Settings** enter the **Account Name** and **Password** for the macOS user account with Secure Token access.
5. Click **Save Changes**.
6. Navigate to your macOS Computer Group and select **Agent Configuration**.



7. In the **Secure Token Enabled Management Credential** field, enter the macOS user credential you created in step 2.
8. Click **Save Changes**.

macOS Privilege Manager Sudo Plugin

Apple's Endpoint Security framework prevents Privilege Manager from performing process elevation of command-line binaries like done in the past. Privilege Manager's previous KEXT support for command line filtering in order to block, elevate, restrict, or allow commands is being replaced with a `sudo` plugin for Apple's newer OS versions starting with Catalina and newer.

Going forward, the `sudo` plugin supports a modular framework that allows third-party policy evaluation to govern whether a command is allowed to run. This architecture allows Privilege Manager to extend `sudo` functionality without replacing it and without introducing too much change to established workflows.

For **existing customers**, if privileged commands are already running via `sudo` and a Privilege Manager policy to elevate it, then there is nothing that needs to be changed. However, if some commands are elevated, specifically via policy and filters, those need to be re-evaluated and modified to utilize `sudo` to perform those commands.

Refer to the macOS Application Approval Process via Sudo Plugin topic. This topic explains the workflow for an approval policy elevating applications executed from a specific folder location.

Policies to elevate the privilege of command-line binaries must contain a **Run as Root** action; this allows them to be distinguished from policies to monitor the execution of command-line binaries.

Sudo Plugin Installation

In support of Big Sur and system extensions, the macOS agent install also installs the macOS sudo plugin at `/usr/local/libexec/sudo`. The plugin is owned by root and its configuration is located at `/etc/sudo.conf`.

macOS Gatekeeper

The macOS Gatekeeper technology can prevent newly downloaded applications and scripts from running, unless downloaded from the App Store or identified as coming from a trusted developer.

Privilege Manager cannot get around these OS specific security protections; however deploying a script that developers use or need to run frequently is possible via the MDM process (and JAMF rollout).

Refer to details as documented by Apple regarding bypassing Gatekeeper via MDM: Gatekeeper and runtime protection in macOS.

System Preferences

On macOS systems, users (Admin and Standard) can customize the System Preferences based on their macOS role scope. System Preferences has been renamed to System Settings in macOS Ventura. Details about macOS-based customizations via System Preferences can be found at https://support.apple.com/guide/mac-help/change-system-preferences-mh15217/mac.

With Privilege Manager, you can implement policies that provide application control to deny execution of all preference panes. Elevation policies are only supported and recommended for management of the following preference panes:

- Battery
- Date & Time
- Energy Saver
- Network
- Lock Screen - Ventura and later - Ventura

The following rules apply for policy managed preference panes:

- If there is no policy for a given preference pane, the authorization aligns with its system default.
- A preference pane's default authorization is restored when an associated policy is disabled/deleted.
- Managed preference pane defaults are restored during an uninstall.

Error Behavior of Preference Panes

When a particular preference pane opens in the System Preferences application, the XPC bundles for that preference pane open. The XPC bundles remain open until the System Preferences application closes completely.

This behavior can result in failed policy evaluations. Opening a preference pane that previously has been opened and evaluated without closing the System Preferences application following the initial opening, results in the policy evaluation not triggering again for that preference pane because the XPC bundle remains open.

For example, if you have a policy that requires approval of Date & Time preference pane changes (and the notification dialog is canceled and Date & Time is re-opened), the notification dialog is not presented to the user again. Instead, a sheet dialog indicates that the preference pane cannot be loaded. To re-trigger policy evaluation, System Preferences must be closed then reopened.

The same thing applies for macOS Ventura, but XPC bundles are no longer used; extensions are used instead. If the notification dialog is canceled, it won't pop up again when trying to change the setting until System Settings is closed and reopened.

User-Based Behavior of Preference Panes

Standard User

Without an active policy, preference panes appear locked, and standard users are unable to make changes. The exception is the Date & Time preference pane. Standard users are allowed to edit the clock appearance. Any changes here are specific to the user's session and can be modified without clicking the locked **padlock** icon, despite the message implication next to the icon.

With an active policy, depending on its action, the following occurs:

- **Deny Execute** | **Deny Execute Message** | **Application Denied** – The system presents users with a dialog indicating they are denied running the preference pane. Depending on the usage of the Deny Execute Message versus the Application Denied Message coupled with the macOS version, each may appear twice.
- **Application Justification** – The system presents users with the justification dialog. Once users enter a justification and click Continue, the system enables all controls on the pane and saves changes. When users click Cancel, macOS displays an error sheet in System Preferences indicating there was an error loading the preference pane.
- **Application Warning** – The system presents users with the warning dialog. When users click Cancel, macOS displays an error sheet in System Preferences indicating there was an error loading the preference pane. When users click Continue, the system enables all controls on the pane and saves changes.
- **Application Approval Request** – The system presents users with the approval dialog. When users click Cancel, macOS displays an error sheet in System Preferences indicating there was an error loading the preference pane. Once users enter a reason and click Continue, the system displays the dialog for waiting for approval. If users click Cancel in the waiting dialog, macOS displays an error sheet in System Preferences indicating there was an error loading the preference pane. Depending on the Approval action (Allow or Deny), the following action occurs:
  - **Allow** – The system enables all controls on the pane and saves changes.
  - **Deny** – macOS displays an error sheet in System Preferences indicating there was an error loading the preference pane.

The following preference panes require admin credentials to make changes and should not be managed with an elevation policy that triggers a user dialog for justification or approvals:

- Parental Controls
- Printers & Scanners
- Security & Privacy
- Sharing
- Time Machine
- Users & Groups

Admin User

Local admin users should not be managed by any policies requiring user interaction when the policy is triggered. For macOS endpoints, the only policy type would be one that demotes administrative rights for a particular preference pane by simply denying access.

Energy Saver and Battery Preference Panes

The Energy Saver Preference Pane is on desktops and the Battery Preference Pane is on laptops.

Beginning with Big Sur, macOS introduced a new preference pane for managing energy-related system preferences for laptop hardware devices. Monterey introduced a new Energy Saver preference pane different from Big Sur and earlier. Additionally, in macOS Ventura, what used to be the Energy Saver Preference Pane on desktops and the Battery Preference Pane on laptops are now split up into the Energy Saver or Battery Preference Pane and the Lock Screen Preference Pane. Because the Energy Saver, Battery, and Lock Screen panes use the same system extension in Ventura and later macOS versions, they must be targeted together.

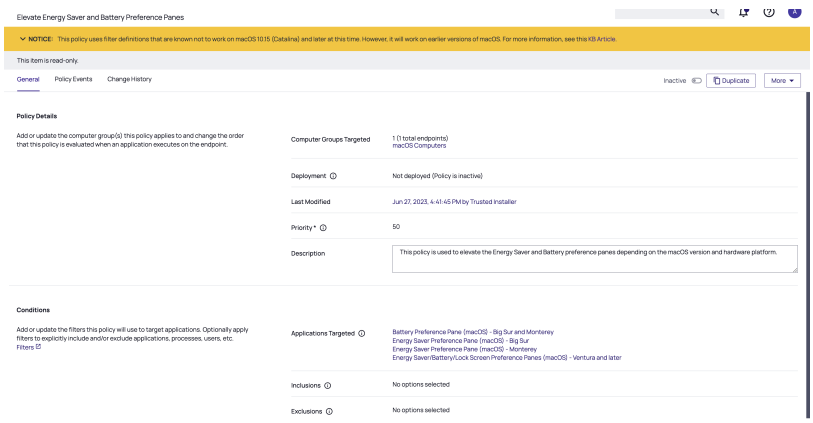
Privilege Manager supports both preference panes with the following filters:

- Battery Preference Pane (macOS) ◆ Big Sur and later
- Energy Saver Preference Pane (macOS) - Big Sur and earlier
- Energy Saver Preference Pane (macOS) ◆ Monterey
- Energy Saver/Battery/Lock Screen Preference Pane (macOS) - Ventura and later

Note: Support for the new Energy Saver/Battery/Lock Screen, Network, and Date & Time Preference panes are available in Privilege Manager agent 11.4.0.

The following default policy is available for direct use. Alternatively, you can duplicate the policy, using it as a template to include an Advanced Message action.

- Elevate Energy Saver and Battery Preference Panes



The policy is configured to elevate without user interaction for the above Battery and Energy Saver preference pane filters such that it is applicable to all macOS versions.

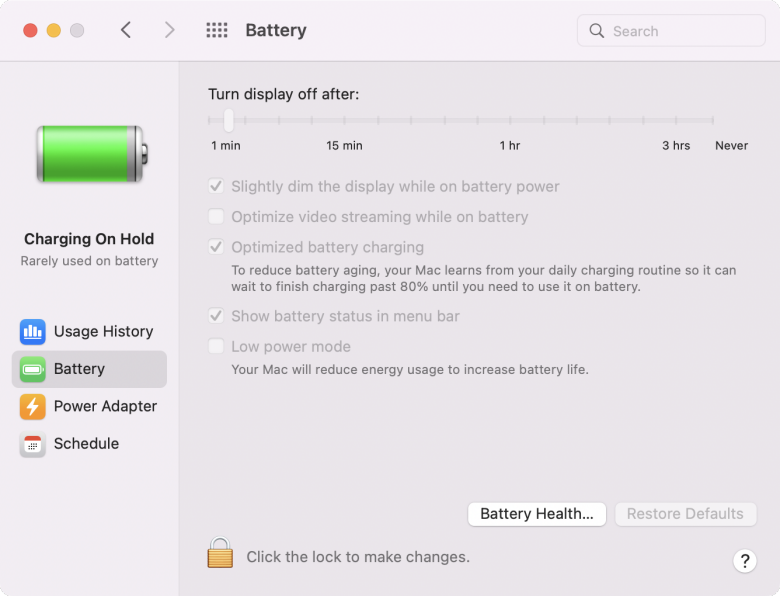
Note: If you have an existing policy that targets Energy Saver and you have macOS Ventura or later endpoints, you must modify the policy to include the **Energy Saver/Battery/Lock Screen Preference Panes (macOS) - Ventura and later** filter. In addition, you must update the Privilege Manager agent on your macOS Ventura and later endpoints to the latest version.

Battery Preference Pane

Standard User - System Defaults

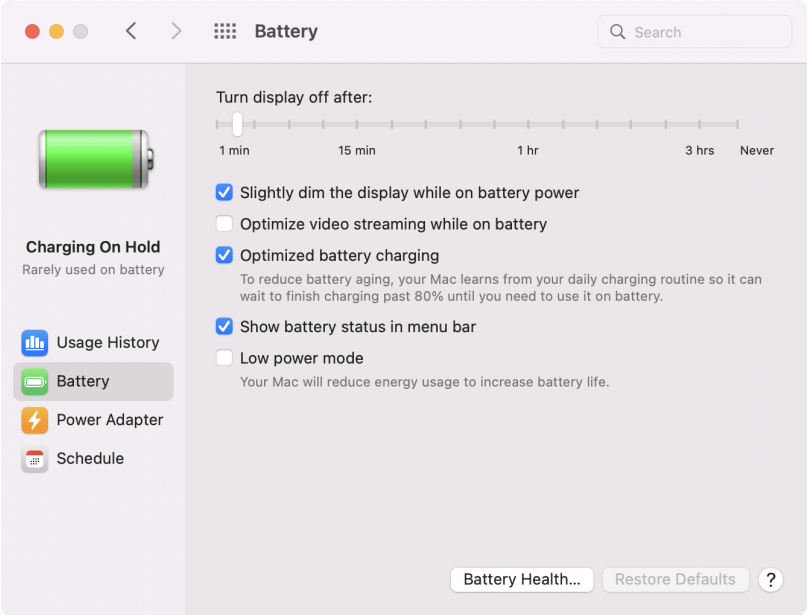
For standard users, when Battery is not managed by a policy, the following conditions apply:

- All controls are disabled and the padlock icon is closed.
- Clicking on the padlock icon results in a prompt, asking for administrator credentials.



Admin User - System Defaults

For admin users, the Battery pane does not have a padlock.

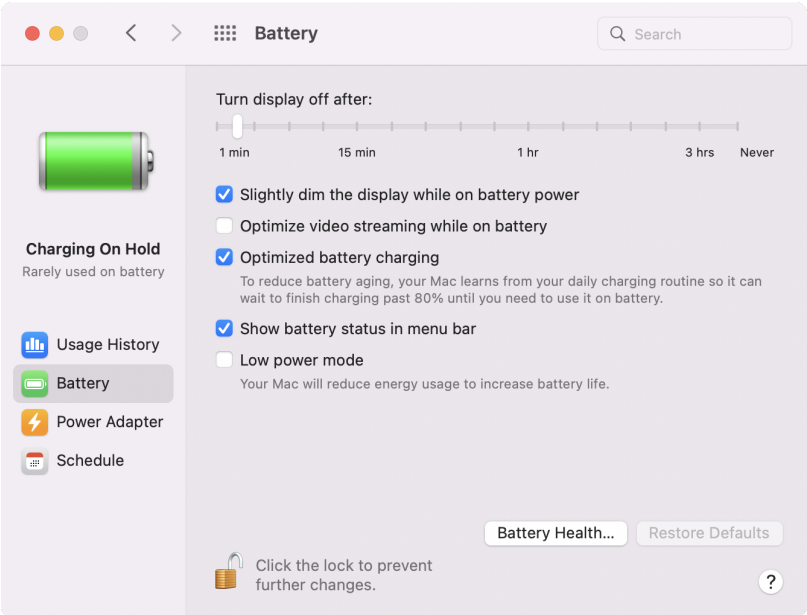


Admin and Standard User - Managed by Policy

For admin and standard users, when Battery is managed by a policy to elevate, the following conditions apply:

- All controls are enabled.
- The padlock icon is not present for admin users and unlocked for standard users.

If the policy includes an advanced message action, the admin and standard users will be prompted accordingly.

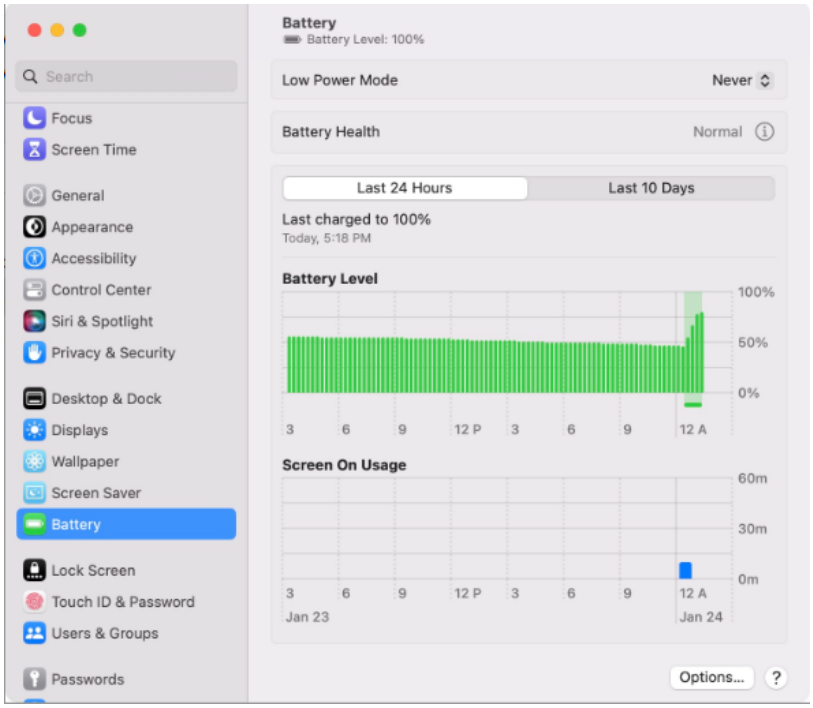


macOS Ventura

In macOS Ventura, System Settings, previously System Preferences, looks much different. There are no longer padlocks that unlock settings. Admin credentials are asked when a user attempts to change individual settings.

Support for targeting the new Battery Preference Pane is available in Privilege Manager Agent version 11.4.0 and Server version 11.4. The Battery pane is shown here.

> **Note:** Battery was split into the Battery and Lock Screen panes in macOS Ventura. See Lock Screen for more information.

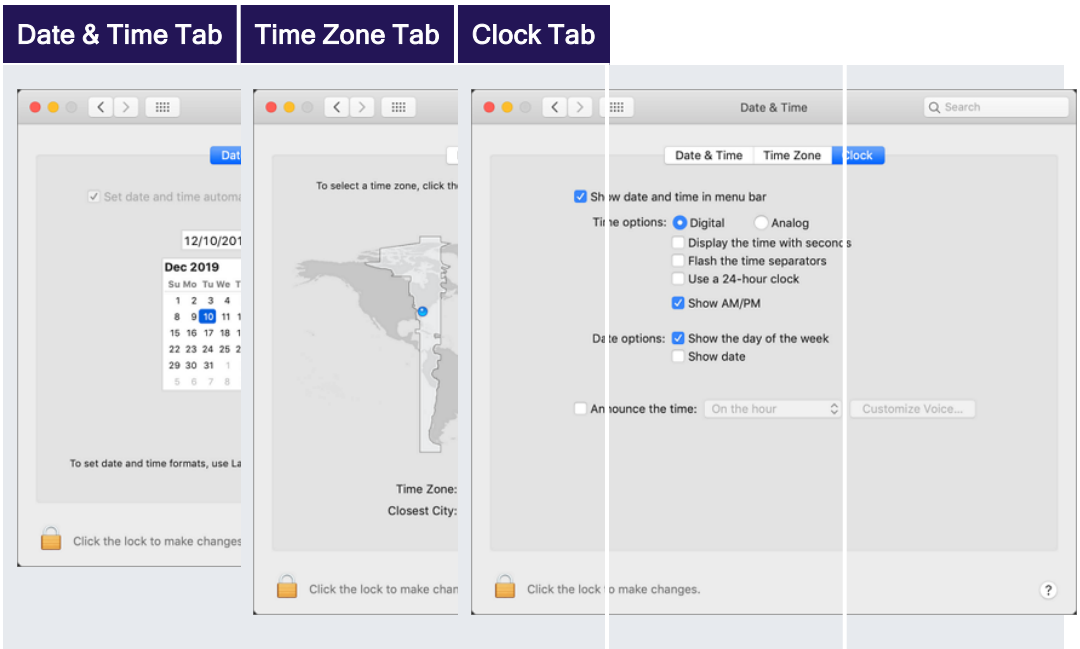


Date & Time Preference Pane

Standard User - System Defaults

For standard users when Date & Time is not managed by a policy, the following conditions apply:

- All controls on the Date & Time tab are disabled and the padlock icon is closed.
- All controls on the Time Zone tab are disabled and the padlock icon is closed.
- All controls on the Clock tab are enabled and changeable by the user. These are user specific settings.
- Clicking on the padlock icon results in a prompt, asking for administrator credentials.

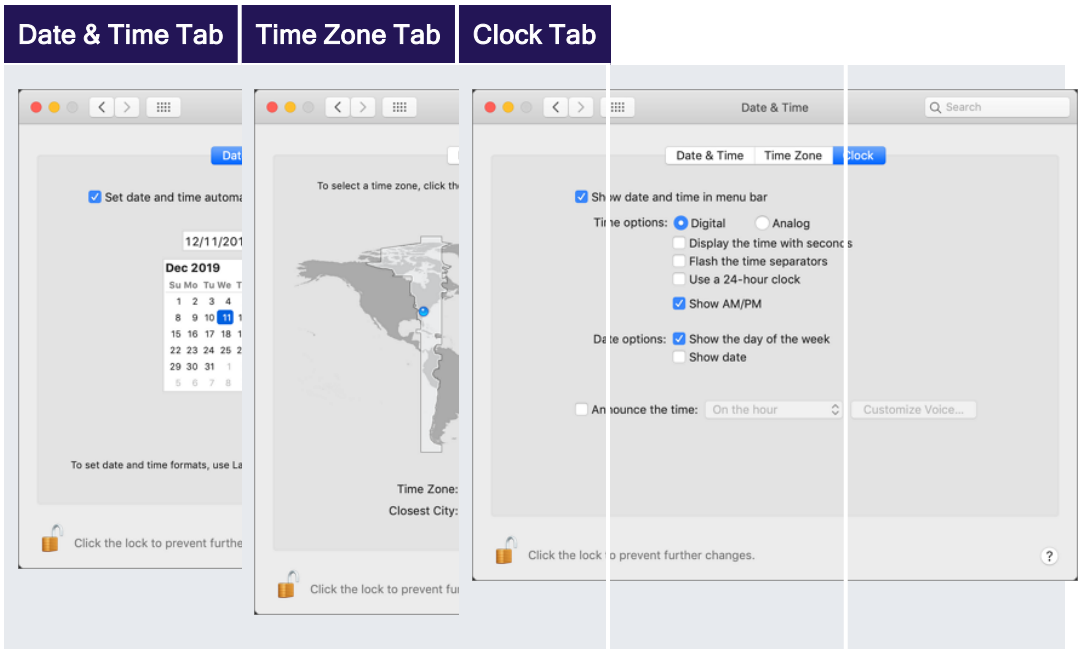


Standard User - Managed by Policy

For standard users when Date & Time is managed by a policy to elevate, the following conditions apply:

- All controls on the Date & Time tab are enabled and changes are saved.
- All controls on the Time Zone tab are enabled and changes are saved.
- All controls on the Clock tab are enabled and changeable by the user. These are user specific settings.
- The padlock icon is unlocked.

Refer to this video demonstration.



Local Administrator User - Not Managed by a Policy

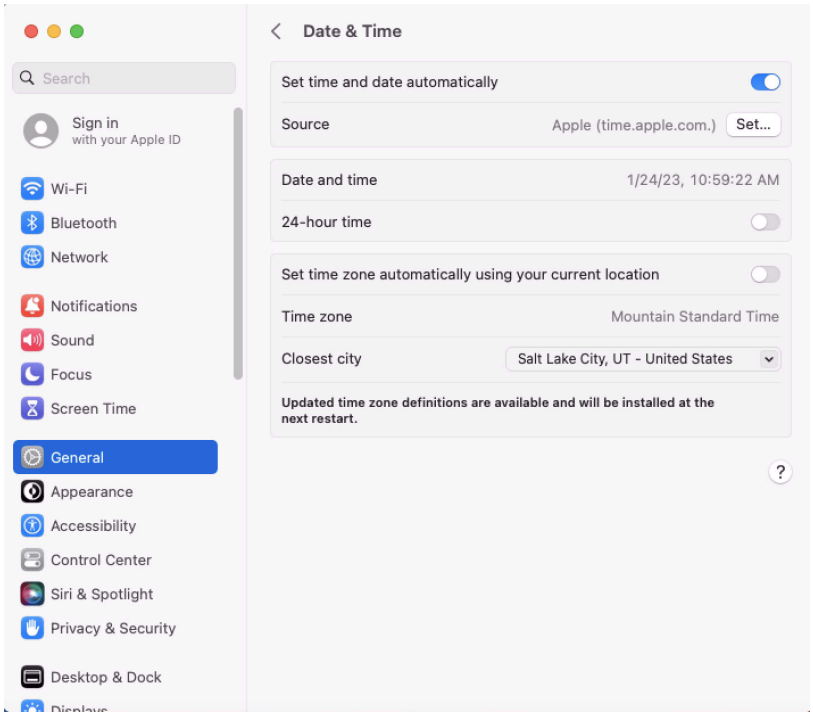
For local admin users, the padlock icon appears locked, by clicking on it a prompt is triggered to enter admin credentials. Once those admin credentials are entered, the padlock icon is unlocked and changes can be made.

Using a policy to run as root is not necessary for local admin users.

macOS Ventura

In macOS Ventura, System Settings, previously System Preferences, looks much different. There are no longer padlocks that unlock settings. Admin credentials are asked for when a user attempts to change individual settings.

Support for targeting the new Date & Time Preference pane is available in Privilege Manager Agent version 11.4.0 and Server version 11.4. The Date & Time pane is in the General tab.



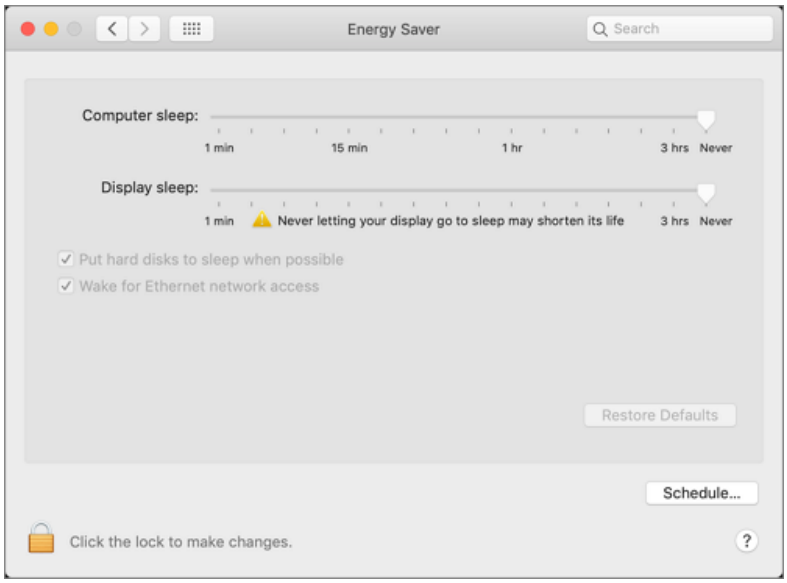
Energy Saver Preference Pane

Standard User - System Defaults

For standard users when Energy Saver is not managed by a policy, the following conditions apply:

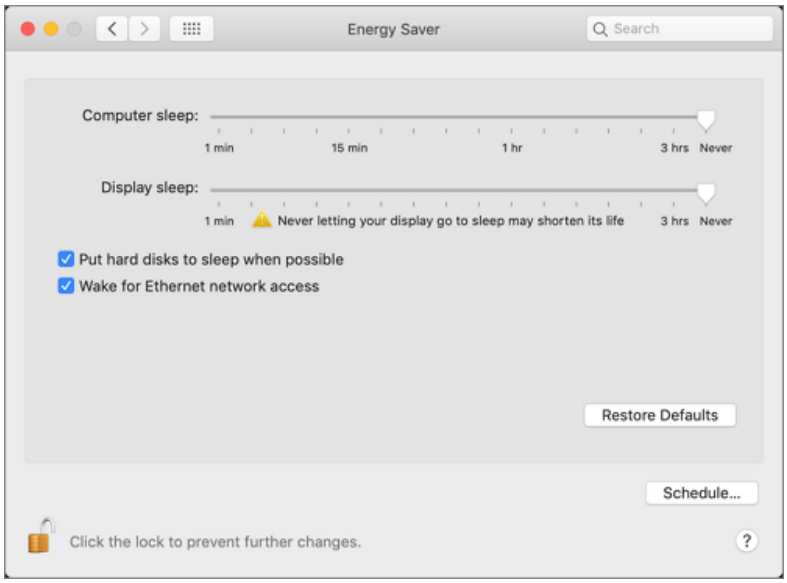
- All controls are disabled and the padlock icon is closed.
- Clicking the Schedule... button shows a panel with disabled controls.

- Clicking on the padlock icon results in a prompt, asking for administrator credentials.



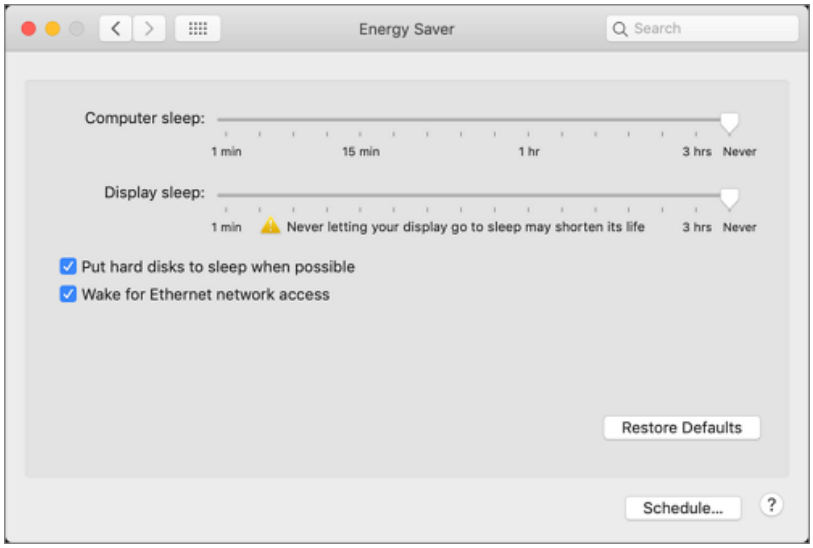
Standard User - Managed by Policy

For standard users when Energy Saver is managed by a policy to elevate, the following conditions apply:

- All controls are enabled and changes are saved.
- Clicking the Schedule... button shows a panel with enabled controls. Any changes are saved.
- The padlock icon is unlocked.
- 

Local Administrator User - Not Managed by a Policy

For local admin users, the Energy Saver pane does not have a padlock and all controls are enabled and changeable. Any changes are saved.

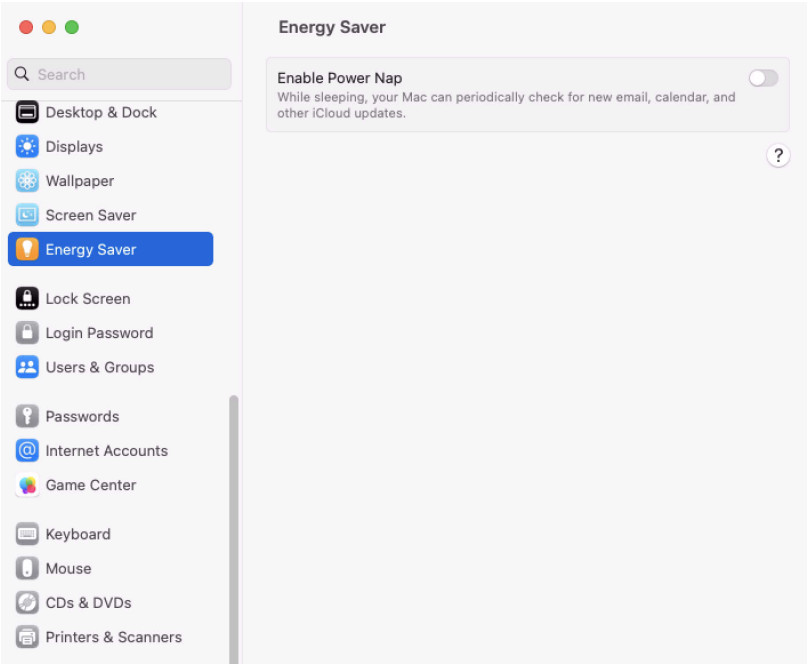


Using a policy to run as root is not necessary for local admin users.

macOS Ventura

In macOS Ventura, System Settings, previously System Preferences, looks much different. There are no longer padlocks that unlock settings. Admin credentials are asked for when you attempt to change individual settings. Support for targeting the new Energy Saver Preference Pane is available in Privilege Manager Agent version 11.4.0 and Server version 11.4. The Energy Saver pane is shown here.

> **Note:** Energy Saver was split into the Energy Saver pane and Lock Screen panes in macOS Ventura. See Lock Screen for more information.



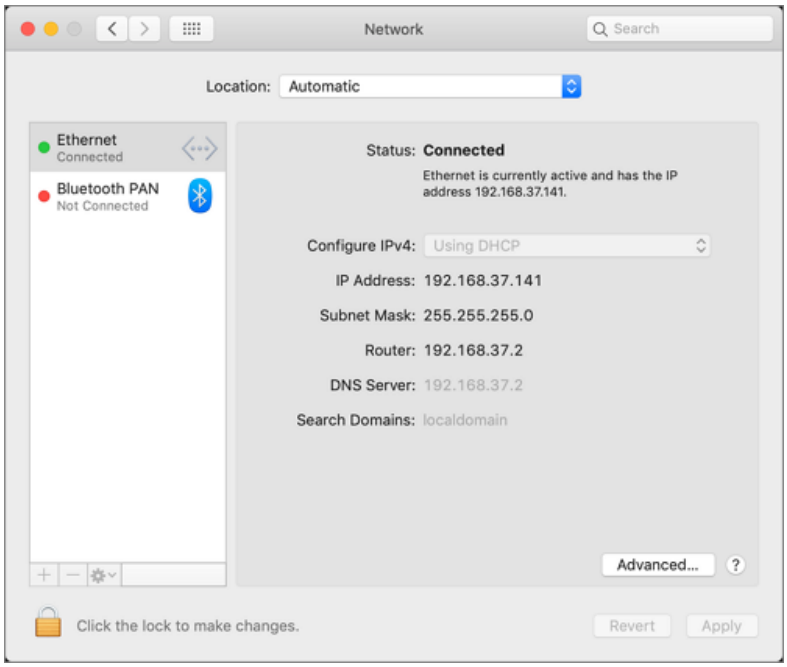
Network Preference Pane

Standard User - System Defaults

For standard users, when Network is not managed by a policy, the following conditions apply:

- All controls except for Location and Advanced are disabled and the padlock icon is closed.
- Clicking the Advanced… button opens a sheet depending on the network interface selected. Based on the selected interface, some elements may be enabled.

- Clicking on the padlock icon results in a prompt, asking for administrator credentials.

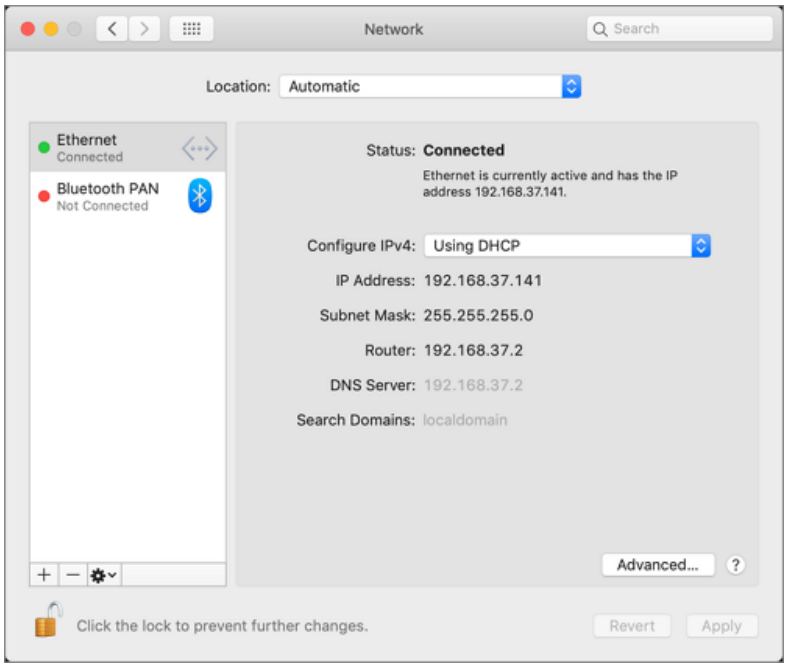


Standard User - Managed by Policy

For standard users, when Network is managed by a policy to elevate, the following conditions apply:

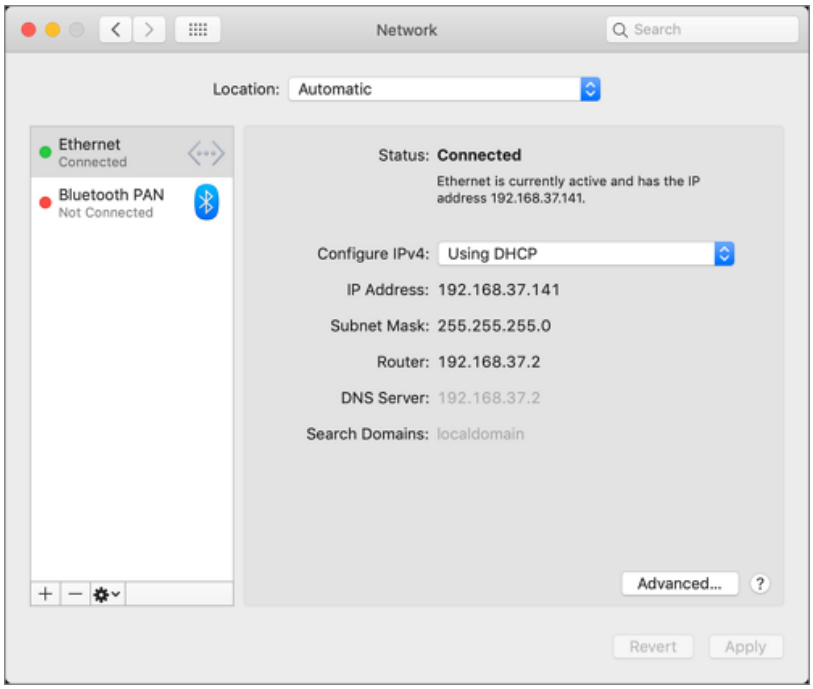
- All controls are enabled and changes are saved.
- Clicking the Advanced... button opens a sheet depending on the network interface selected. Based on the selected interface, elements are enabled.

- The padlock icon is unlocked.



Local Administrator User - Not Managed by a Policy

For local admin users, the Network pane does not have a padlock and all controls are enabled and changeable. Any changes are saved.



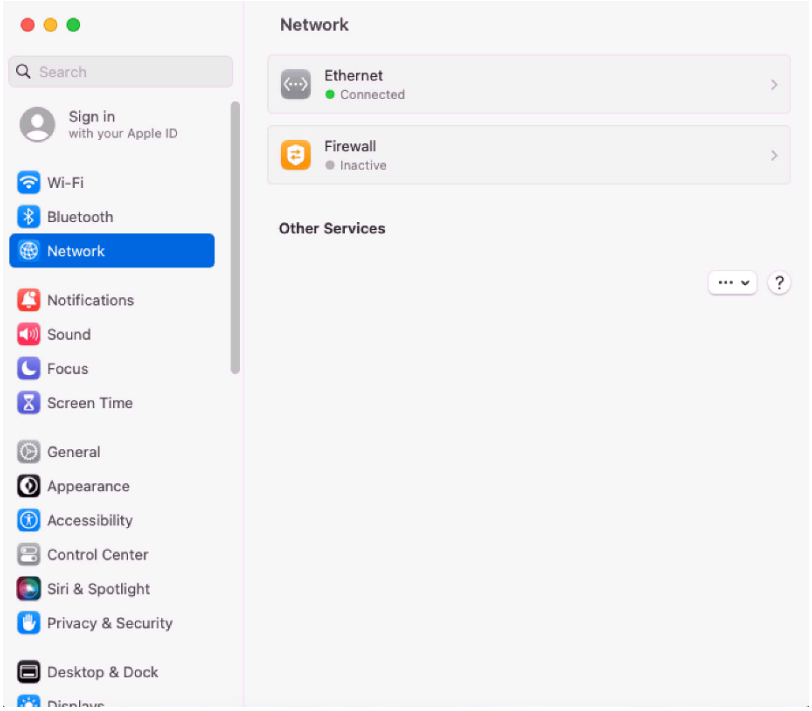
Using a policy to run as root is not necessary for local admin users.

macOS Ventura

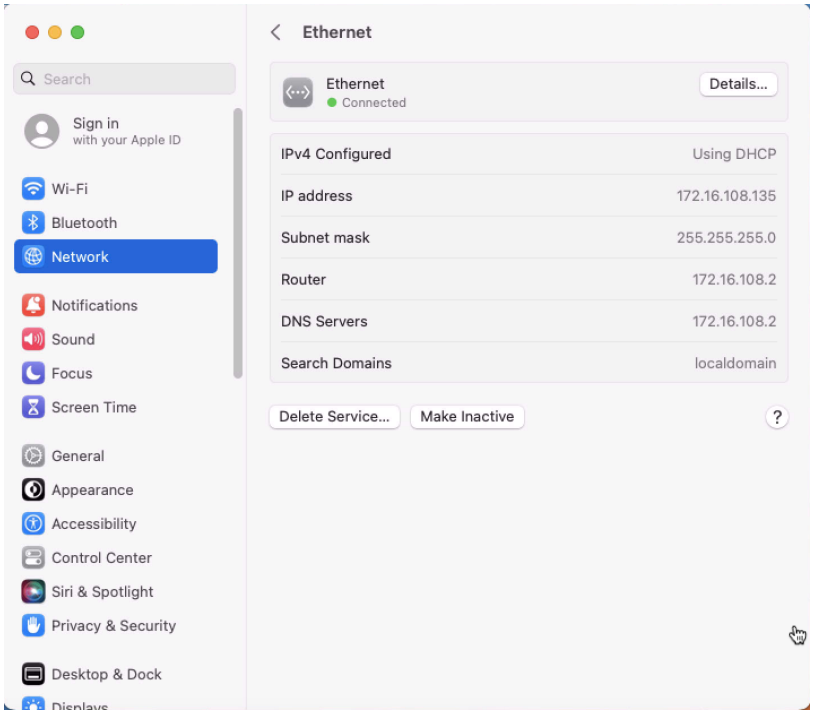
In macOS Ventura, System Settings, previously System Preferences, looks much different. There are no longer padlocks that unlock settings. Admin credentials are asked for when a user attempts to change individual settings.

Support for targeting the new Network Preference Pane is available in Privilege Manager Agent version 11.4.0 and Server version 11.4. The Network Preference Pane is shown here.

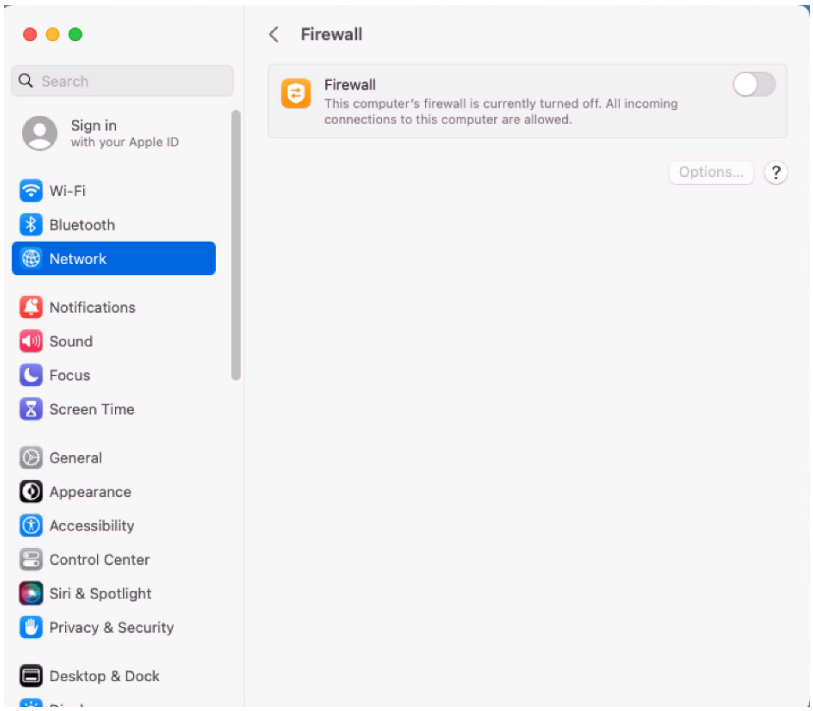
From here, click **Ethernet** or **Firewall**.



Ethernet Connection



Firewall Turned On



Printer Installs

To install and manage printers via the Printers and Scanners preference pane, standard users on macOS should be added as members of the **lpadmin** group. Refer to this example video.

On macOS, adding a printer can happen in three ways. Two of those are allowed through an elevation policy, enabling a user to add a printer with either:

- an .app installation file directly
- a .pkg driver installation directly

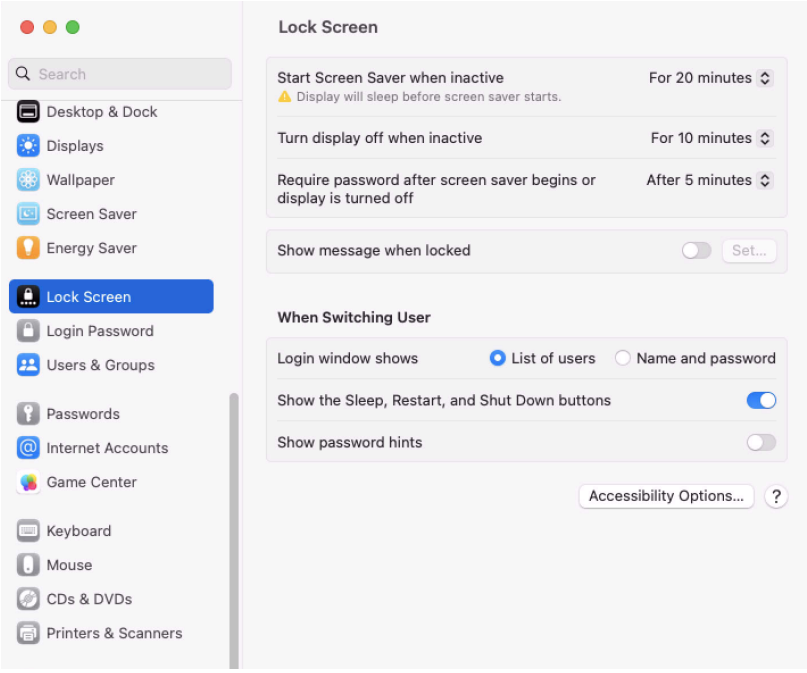
The third option is where the Printers and Scanners preference pane is used to manually add a printer based on existing printer drivers. Refer to the link below for more information.

Under the first scenario, the application that is performing the install and configuration of the printer may prompt for admin credentials. If this is the case, you may need a policy that allows the application or applications provider by the printer vendor.

Refer to https://support.apple.com/guide/mac-help/add-a-printer-on-mac-mh14004/10.15/mac/10.15 for the latest printer setup information from Apple.

Lock Screen Preference Pane

The Lock Screen Preference Pane was introduced in macOS Ventura. This information was previously incorporated into the Energy Saver or Battery Preference Panes.



Standard User - System Defaults

For standard users when Lock Screen is not managed by a policy, the following conditions apply:

- All controls except for **Start Screen Saver when inactive** need admin credentials.
- Clicking **Accessibility Options** opens a page with accessibility options that require Admin credentials. (Note that you will be prompted for your Admin credentials, when required.)

Standard User - Managed by Policy

For standard users, when Lock Screen is managed by a policy to elevate, the following conditions apply:

- All controls are enabled and changes are saved.
- Clicking **Accessibility Options** opens a page with accessibility options, which are enabled.

Local Administrator User - Not Managed by a Policy

For local admin users, all controls on the Lock Screen are enabled.

Privilege Manager on Windows

Once Privilege Manager is added to a companies infrastructure, it discovers all accounts that exist on endpoints and allows Privilege Manager Administrators to control the exact membership of every local group via its Local Security features. This ensures the correct admin and root accounts are permanently set. Additionally, credentials will be controlled by enforcing password rotation on those accounts.

Privilege Manager's Application Control allows administrators to manage application activity on endpoint machines. Applications that require admin rights or root access can be automatically elevated, allowed applications are allow listed, and malicious applications are blocked.

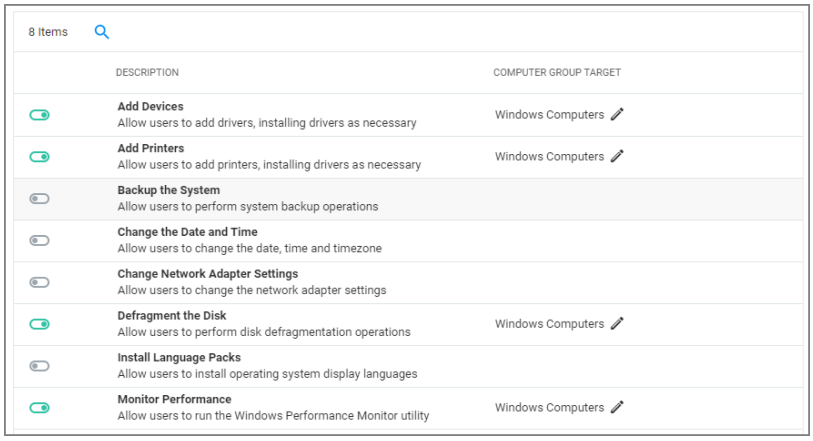
Specific to the Windows Operating systems are the management of:

- Client System Settings
- Adjust Process Rights Action

Client System Settings

The Client System Settings are common settings for standard Windows endpoint systems ranging from allowing installation of drivers to printers. These settings are deployed to Agents the same as any Policy.

By default each setting targets the default "Windows Computers" Computer Group.



Changes to client system settings do not take effect until Policies have been cached and deployed to the agent. Review the agent status reports to see which agents have which Policies.

Add Devices

If active, users on Windows endpoints are allowed to add and install device drivers.

Add Printers

If active, users on Windows endpoints are allowed to add and install printer drivers.

Backup the Systems

If active, users on Windows endpoints are allowed to perform system backup operations.

Change the Date and Time

If active, users on Windows endpoints are allowed to change date, time, and timezone settings.

Change Network Adapter Settings

Note: In order to implement this functionality, the UAC settings in Windows 10 operating systems (C:\Windows\System32\UserAccountControlSettings.exe) must be enabled.

If active, users on Windows endpoints are allowed to change network adapter settings.

On Windows 7 endpoints with **Change Network Adapter Settings** active, do NOT enable high integrity when using the Administrative Rights action in policies.

Defragment the Disk

If active, users on Windows endpoints are allowed to perform disk defragmentation operations.

Install Language Packs

If active, users on Windows endpoints are allowed to install operating system display language packs.

Monitor Performance

If active, users on Windows endpoints are allowed to run the Windows Performance Monitor Utility.

Agents

The Privilege Manager Agents are a critical component of Delinea's application control and local security, giving you the ability to evaluate the health and status of endpoints in real time. Agents are required on endpoint machines to implement Privilege Manager policies.

Privilege Manager provides pre-configured and fully customizable reporting on the status of agents and endpoint operating systems. In the Privilege Manager reporting dashboard, you can drill into reports based on any dimension and easily export report data to other reporting applications or Excel.

Privilege Manager supports agents on these workstations:

- Windows
- macOS

For information about installing agents, refer to Agent Installation to review agent system requirements and the specific agent installation procedures. This section of our document is a general agent information section, containing details about how to use/interact with agents and to provide information about the agent processes.

Agent Hardening

Windows Endpoints

To make sure that local Administrators do not tamper with Delinea agents running on their system, Privilege Manager Administrators can define users that can start and stop the Privilege Manager services running on endpoints, such as the Delinea Agent or Delinea Application Control. Refer to Agent Hardening.

macOS Endpoints

It is not currently possible to prevent a local administrator account on macOS from starting and stopping a background service like the Privilege Manager agent. Refer to macOS Agent Hardening for best practices.

Post Agent Installation

When your agents are installed, you can verify the status of your Agents' health in terms of Registration State and Policy State from the Home page. You also can navigate to **Admin | Agents** for more information about installed agents.

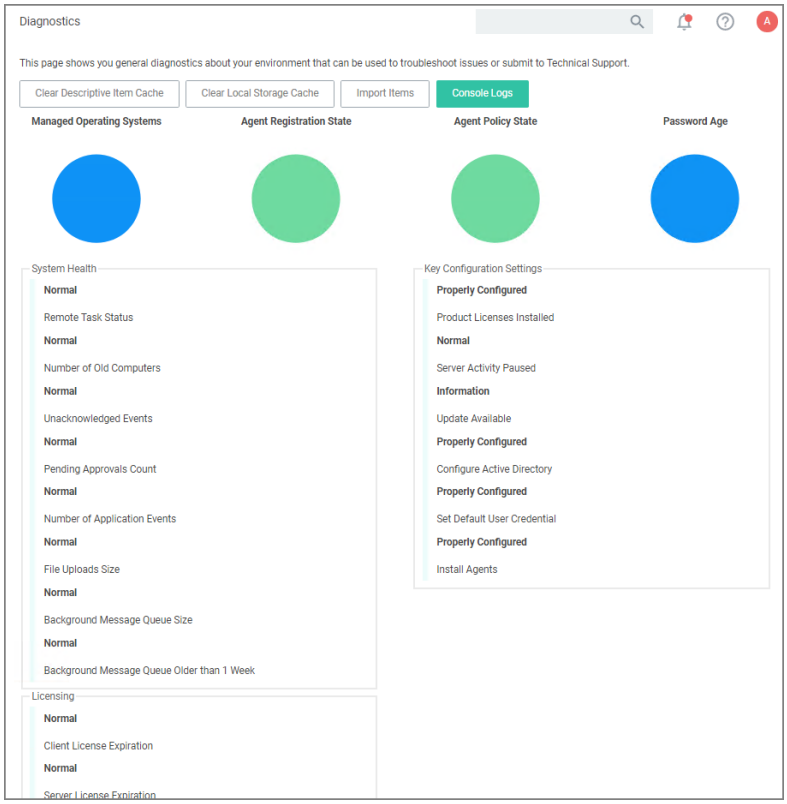
The Agent Health dials describe how many Managed Operating Systems you have as well as your Agent(s) Registration State and Policy State. If you click on the Agent Registration State dial, you will see a report on a list of machines (the "MonitoredResource" column) where each registered agent is installed.

Clicking the Agent Policy State dial from the Home dashboard brings you to a report that links all of your agent-registered machines with the Number of Policies Missing from each agent. This page will become invaluable once you have multiple policies running over different computer groups in your network.

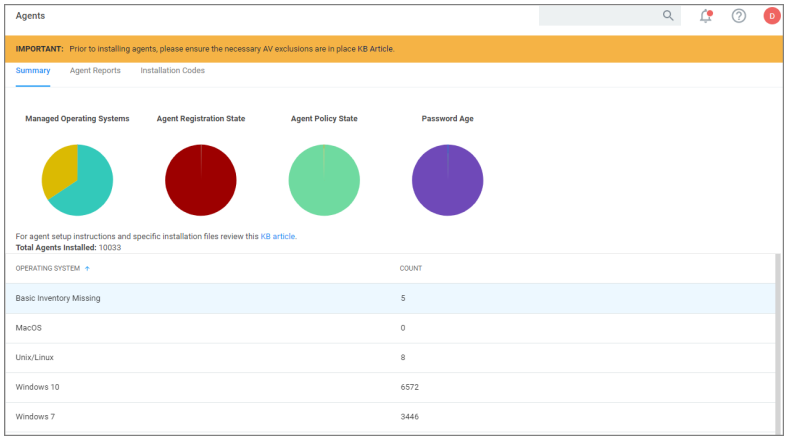
Agent Diagnostics

Once your agents are installed, verify that they have registered in Privilege Manager. Navigate to either:

- **Admin | Diagnostics** to access the **Diagnostics** page or

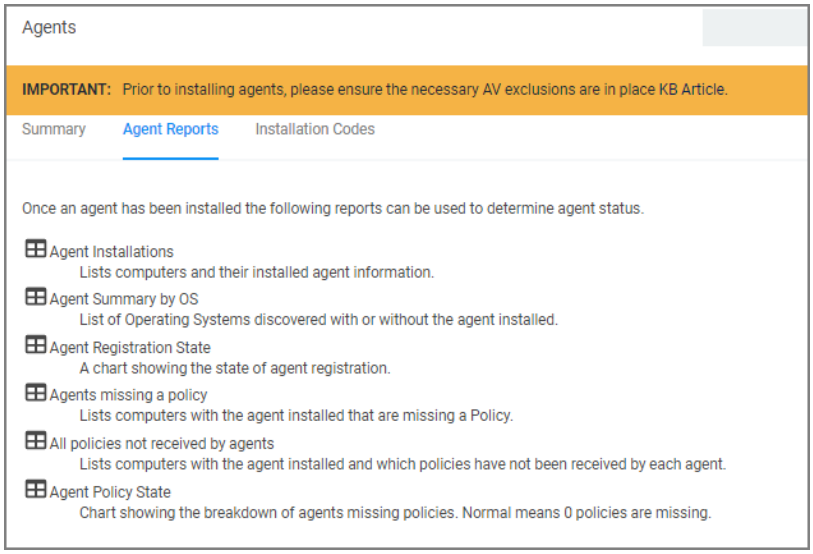


- **ADMIN | Agents** to view your agent details.

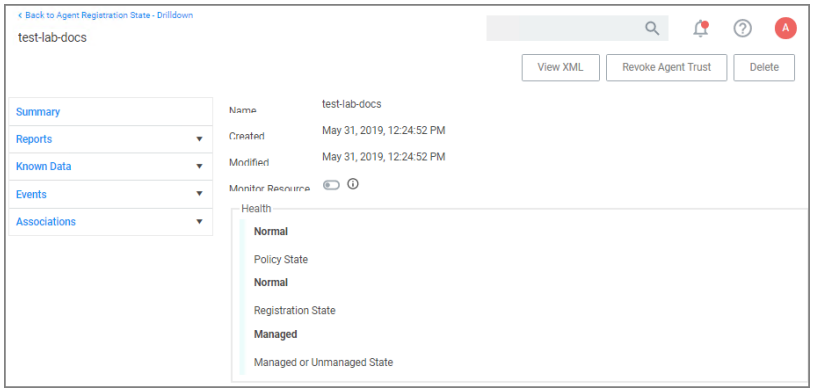


After the initial policies are received, future updates will be based on the task schedules set in Update Applicable Policies and Scheduled Registration policies. Ensure to select the correct policies based on Windows or Mac operating systems. To edit these schedules, navigate to your computer group and select **Scheduled Jobs**. The **Triggers** can be customized under the **Job Schedule** section.

On the agent details page you will see the quantity of agents registered and what operating system is running on registered endpoints. Registered endpoints can also be viewed in the report **Agent Installation Summary** by navigating to the **Agent Reports** tab.



From the the reports pages you can click into any of the **target machines** listed that have a Delinea agent installed. Pictured below is a view from one of these resource pages where you can check the machine's System Health and configured policies.



Agent Encryption

The agent traffic is secured via SSL/TLS (1.2).

Elevated Processes

Starting with Privilege Manager version 10.8.2, the agent adds memory checks for all processes that are managed/elevated via Privilege Manager. Any processes not managed by Privilege Manager, should be checked for process hollowing through means of products like Windows Defender ATP.

Pertaining to All Agents

This section of the Privilege Manager documentation covers information and step procedures pertaining to Privilege Manager agents **independent** of the endpoint operating system.

The following topics are available:

Setting the Privilege Manager Server Address

Agents require a Privilege Manager Server to communicate with. The recommended way to set the URL address is during the installation of the Delinea Agent. If an Azure Service Bus or Reverse Proxy is used, the URL can point at the URL of those components.

Setting the Privilege Manager Server Address for macOS

On a macOS agent, you can set the server address using the command line or the Privilege Manager settings pane. Either method requires administrative privileges.

Command Line

Open a terminal window, enter the following command:

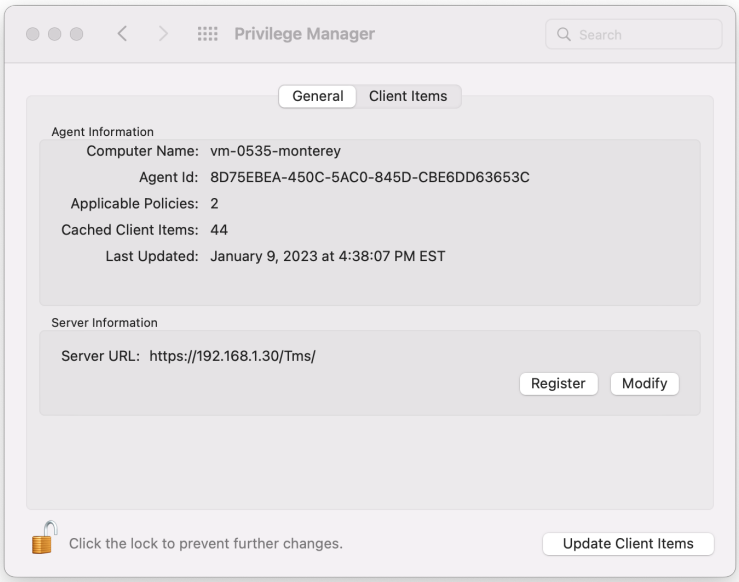
```
pmagentctl server --url https://<server address>/Tms/
```

A dialog appears. Enter your administrator credentials.

Privilege Manager Settings

Access System Preferences (or System Settings for macOS Ventura) and select **Privilege Manager**.

Click the lock icon and enter administrator credentials to unlock and allow changes. Click **Modify** and enter the server address.



Setting the Privilege Manager Server Address for Windows

The URL address can be changed post-install via the registry or PowerShell.

Setting the Privilege Manager Server (TMS) Address via PowerShell

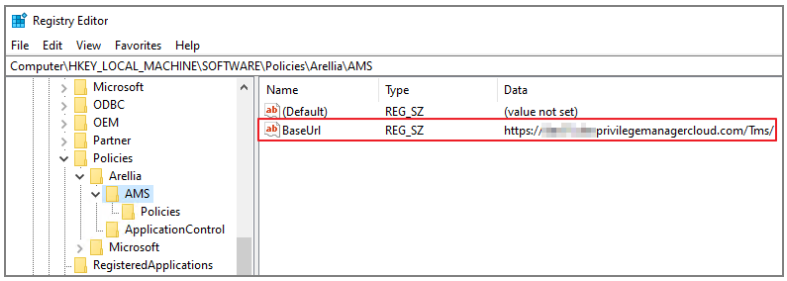
To set the Privilege Manager Server (TMS) address via PowerShell, run this command as Administrator:

```
C:\Program Files\Thycotic\Powershell\Arellia.Agent\SetAmsServer.ps1
```

The script will then ask you to type in the fully qualified domain name of the server.

Changing the Privilege Manager Server (TMS) Address via the Registry Editor

1. Open the Registry Editor (regedit)
2. Navigate to **HKEY_LOCAL_MACHINE | SOFTWARE | Policies | Arellia | AMS**.
3. Right click BaseUrl and select Modify.



4. In the Edit String dialog box, change the BaseURL to your TMS Address.
5. Close the registry.
6. Restart the Agent service.

Agent Specific Tasks

Certain Privilege Manager tasks are directly related to agent processes and their operational loads.

Server side tasks, also known as Remote Client Scheduled Commands do not require a policy. Agent tasks require a policy. These types of tasks are with the exception of one, by default enabled and run on a scheduled basis. Most are read-only system tasks, that can be copied, renamed, and then customized.

The majority will run for the first time after system initialization.

Windows Remote Client Scheduled Commands

Name	Description	Schedule	Enabled
Restrict Account Permissions on Agent Services (Windows)	Instructs computers to only allow the specified users to start and stop the Delinea services.	n/a	No
Basic Inventory (Initial, Windows)	Instructs computers to report the Win32_ ComputerSystem, Win32_ComputerSystemProduct and Win32_OperatingSystem WMI classes to the server.	daily	Yes
Basic Inventory (Windows)	Instructs computers to report the Win32_ ComputerSystem, Win32_ComputerSystemProduct and Win32_OperatingSystem WMI classes to the server.	daily	Yes
Cleanup Agent Inventory Transfers (Windows)	Completes and cleans BITS transfers and temporary files used by the TMS Agent Inventory Helper.	daily	Yes
Cleanup sent Privilege Manager Events (Windows)	Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.	daily	Yes
Configure Privilege Manager Remove Programs	Configure the Privilege Manager Remove Programs behavior.	daily	Yes
Default File Inventory Policy (Windows)	The purpose of this policy is to inventory software programs running on the managed computer.	weekly	Yes

Agents

Name	Description	Schedule	Enabled
Deploy File Hash Exclusion Setting (Windows)	The purpose of this policy is to provide the ability to exclude certain file extensions from the hash process.	daily	No
Ensure UAC Override Setting (Windows)	Ensures that the UAC Override Registry Key is set.	daily	Yes
Local User Inventory Policy	The purpose of this policy is to inventory Local User account, groups and group membership on the client. This policy can also be used to inventory for specific account privileges.	weekly	Yes
Perform Resource Discovery (Windows)	Schedule on which agents will check with server to determine if any local resources require discovery.	daily	Yes
Retry errored TMS Events (Windows)	Scan Agent queue for any events that require retransmission.	daily	Yes
Scheduled Check Pending Client Tasks - Internet Clients (Windows)	Initiate a check for pending client tasks. Used by agents that are unable to receive an incoming connection from the server.	daily	Yes
Scheduled Registration - Internet Clients (Windows)	Initiate agent registration with server less frequently than internal clients.	daily	Yes
Scheduled Registration (Windows)	Initiate agent registration with server.	daily	Yes
Update Agent Commands (Windows)	Instructs Agent to update any agent commands if required.	daily	Yes
Update Applicable Policies - Internet Clients (Windows)	Instructs Agent to check with server for policy changes.	daily	Yes
Update Applicable Policies (Windows)	Instructs Agent to check with server for policy changes.	daily	Yes
Update Provisioned Resource Client Items (Windows)		daily	Yes

Name	Description	Schedule	Enabled
User Logon Inventory Policy	Updates user logon data on the given schedule.	weekly	Yes
Windows Service Inventory Policy	The purpose of this policy is to inventory Windows Services on the client.	weekly	Yes

macOS Remote Client Scheduled Commands

Name	Description	Schedule	Enabled
Basic Inventory (Initial, macOS)	This scheduled task triggers the Agent to send macOS basic inventory.	daily	Yes
Basic Inventory (macOS)	This scheduled task triggers the Agent to send macOS basic inventory.	daily	Yes
Cleanup sent Privilege Manager Events (macOS)	Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.	daily	Yes
Default File Inventory Policy (macOS)	The purpose of this policy is to inventory software programs running on the managed computer.	weekly	Yes
Ignore macOS Catalina software update (macOS)	The purpose of this policy is to provide a way in Privilege Manager to ignore macOS updates.	daily	no
Local User Inventory Policy (macOS)	The purpose of this policy is to inventory Local User account, groups and group membership on the client. This policy can also be used to inventory for specific account privileges.	weekly	Yes
Perform Resource Discovery (macOS)]	Schedule on which agents will check with server to determine if any local resources require discovery.	daily	Yes
Reset ignored macOS software updates (macOS)	The purpose of this policy is to provide a way in Privilege Manager to reset ignored macOS updates.	daily	No
Retry errored TMS Events (macOS)	Scan Agent queue for any events that require retransmission.	daily	Yes

Name	Description	Schedule	Enabled
Scheduled Registration (macOS)	When this policy is triggered the Agent will attempt (or re-attempt) to register with the server.	daily	Yes
Update Agent Commands (macOS)	When this policy is triggered the Agent will update agent command items.	daily	Yes
Update Applicable Policies (macOS)	When this policy is triggered the Agent will check the server for updated policies.	daily	Yes
Update Provisioned Resource Client Items (macOS)		daily	Yes

Unix/Linux Remote Client Scheduled Commands

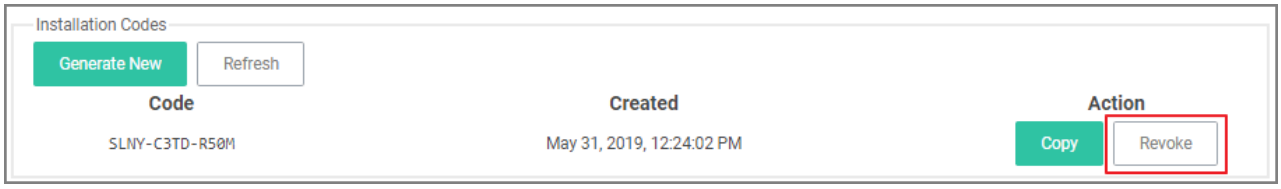
Name	Description	Schedule	Enabled
Basic Inventory (Initial, Unix/Linux)	This scheduled task triggers the Agent to send initial Unix/Linux basic inventory.	daily	Yes
Basic Inventory (Unix/Linux)	This scheduled task triggers the Agent to send Unix/Linux basic inventory.	daily	Yes
Remove Successful Agent Events (Unix/Linux)	This command will remove agent events that have been successfully uploaded to Privilege Manager.	daily	Yes
Scheduled Registration (Unix/Linux)	This agent-scheduled task refreshes registration data for the assigned agents.	daily	Yes
Update Applicable Policies (Unix/Linux)	This remote-scheduled command will update policies applicable to the assigned agents.	daily	Yes

Agent Trust Revocation

With Privilege Manager 10.5 and up, you can revoke an agent trust relationship.

Revoking the Trust from the Server

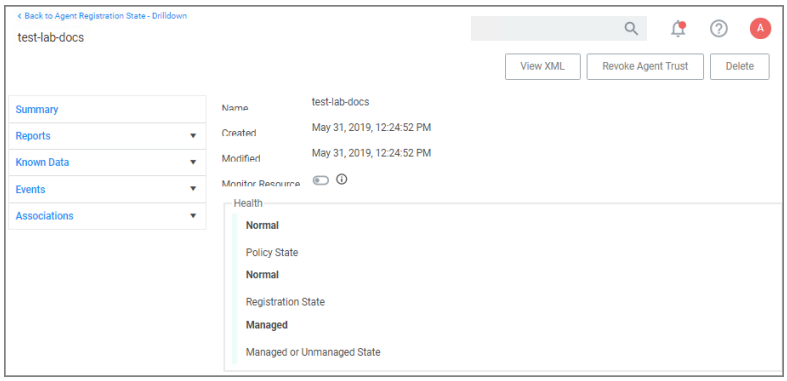
1. Navigate to the Agent Install Code's page and click **Remove Agent Trust**.



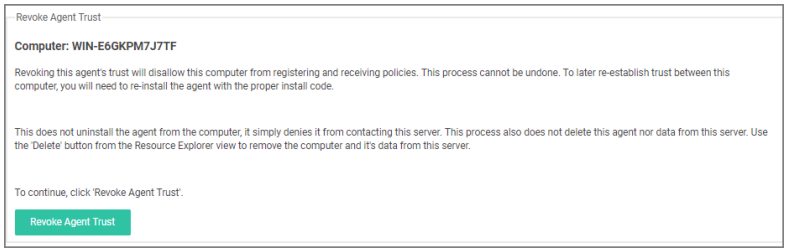
2. Click **OK** to confirm.

Revoking the Trust for the Computer Resource

1. Navigate to **Admin | Agents** to open the Agents Summary page.
2. Select an Operating System group from list.
3. On the Managed Computers by Operating System page, select one of the computer resources.



4. Click **Revoke Agent Trust**.



5. Confirm by clicking **Revoke Agent Trust**.

Message on the Revoke Agent Trust dialog:

Revoking this agent's trust will disallow this computer from registering and receiving policies. This process cannot be undone. To later re-establish trust between this computer, you will need to re-install the agent with the proper install code.
This does not uninstall the agent from the computer, it simply denies it from contacting this server. This process also does not delete this agent nor its data from this server. Use the 'Delete' button from the Resource Explorer view to remove the computer and it's data from this server.

Agent Uninstall Script

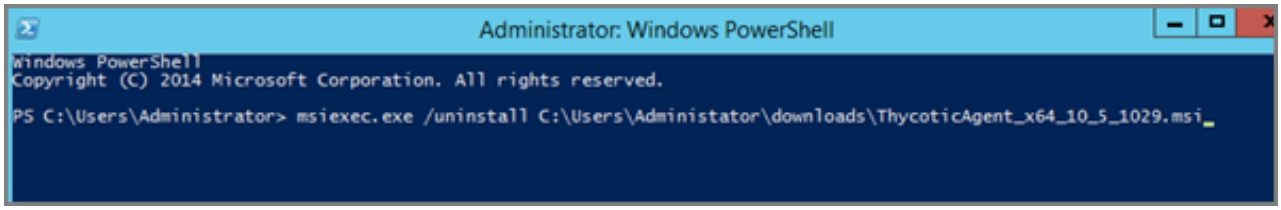
This topic covers uninstalling an agent when the endpoint is not going to be upgraded to a new version of Privilege Manager agents anymore.

If you're trying to uninstall an old agent in order to install a newer version of the agent, use the Upgrade Products/Feature link under the Setup page.

Using a PowerShell Script to Uninstall an Agent

1. Navigate to the machine(s) where the agent is located.
2. Right-click on **Windows Powershell** and **Run as administrator**.
3. Run the following command:

```
msiexec.exe /x ThycoticAgent_x64_VERSION.msi /qn
```



4. On the prompt, click **Yes**.

Addressing Invalid Agent Registrations

When agents are failing to register because they are unknown or have an invalid install code, an alert will be raised in Privilege Manager. The alert has a link to a report that shows key details such as name and source IP.

Privilege Manager Admins should review the list of invalid registrations and determine whether the computer needs to have the agent re-registered, or removed completely.

When the agent is later registered properly, the Invalid Registration record will be removed from the alerts and the report (after the **Update Server Gauge** task has been run).

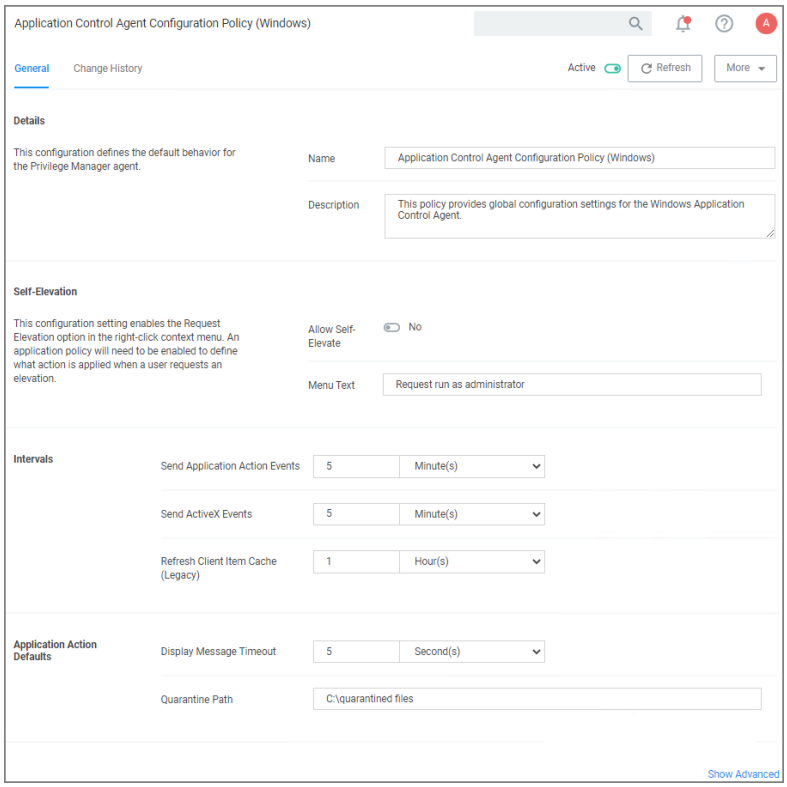
If the invalidly registered agent is removed from the reported computer, Privilege Manager Admins can run a new task, called **Purge Maintenance - Invalid Agent Registrations** to clear down the computers that have been addressed.

Note: The parameter on this report defaults to computers that have had Invalid Registrations for more than 90 days, so this can be changed to zero if there have been a lot of invalid registrations to clear down.

Configuring for a Test Environment

You need to set Privilege Manager Agent configuration options to readily test configuration changes in a test environment. The agent configurations outlined in this page allow for accelerated feedback when testing use cases.

1. Under your Computer Group select **Agent Configuration**.



2. Under Self-Elevation, set the Request Elevation option. For this an application policy needs to be enabled to define what action is applied when a user requests an elevation. Enter the text for the message in the text field.
3. Under Intervals, adjust the values to receive quicker turnarounds on any tests run on a test instance.
   a. Set Sent Application Action events every to 1 Minutes.
   b. Set Send ActiveX events every 5 Minutes.
   c. Set Refresh Client Items cache every 5 Minutes.
4. Set the **Application Action Defaults**, like the Display Message Timeout and Quarantine Path.
5. Keep the advanced settings as is (Delinea recommends to only change the advanced settings after consulting via Professional Service engagement.)
6. Click **Save Changes**.

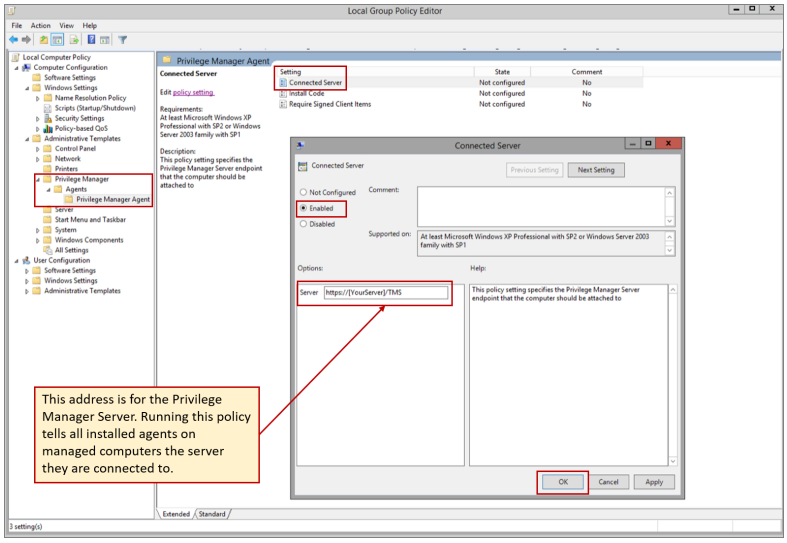
Connecting Agents to the Privilege Manager Server via Group Policy

Regardless of how you installed agents or rolled agents out to your network, Privilege Manager has a method to link those agents with Servers. Privilege Manager has templates (files) that enable you to point agents back to the

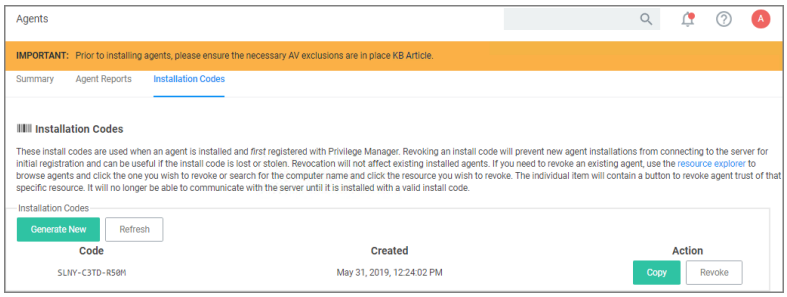
Privilege Manager Server.

To perform this task, do the following steps:

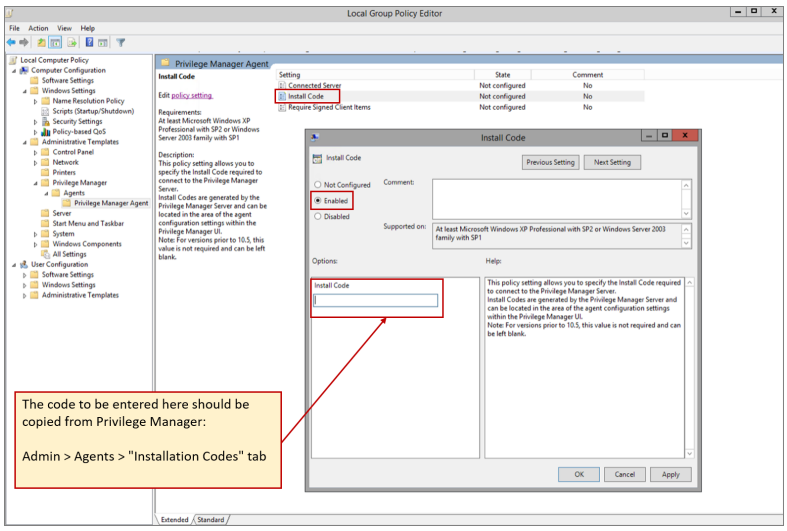
1. Download the attached PrivilegeManagerAgent.admx and PrivilegeManagerAgent.adml zip folders and extract the corresponding files (one file from each zip folder).
2. Install the downloaded and extracted custom Privilege Manager Group Policy files either on a single machine or on a domain controller.
   - To install on a single machine:
     a. Copy PrivilegeManagerAgent.admx to `%systemroot%\PolicyDefinitions`
     b. Copy PrivilegeManagerAgent.adml to `%systemroot%\PolicyDefinitions\en-US`
   - To install on a Domain Controller effectively making the custom GPO available to all Domain Administrators:
     a. Copy PrivilegeManagerAgent.admx to `%systemroot%\SYSVOL\domain\Policies\PolicyDefinitions`
     b. Copy PrivilegeManagerAgent.adml to `%systemroot%\SYSVOL\domain\Policies\PolicyDefinitions\en-US`
3. From the Group Policy Management Editor, navigate to Policies.
4. Go to Administrative Templates > Privilege Manager > Agents > Privilege Manager Agent and click Connected Server.



5. In the Connected Server window click **Enabled**.
6. In the Server field, **enter** the **URL** for your Privilege Manager Server, click **OK**.
7. Now you need to copy some data from Privilege Manager. In Privilege Manager, navigate to **Admin | Agents | Installation Codes** tab.



8. Copy the **Code** value by clicking **Copy**.
9. Switch back to the Group Policy Editor, in the Privilege Manager Agent window, click Install Code.



   a. In the Install Code window, click **Enabled**.
   b. In the Install Code field, paste the Code value you copied from Installation Codes tab in Privilege Manager.
   c. Click **OK**.
10. Set the Client Item Signature Validation. By default, Privilege Manager validates only client items that have a signature present. If you want to require that all client items have a valid signature, then configure the group policy settings to enforce the **Require Signed Client Items** setting.

Un-Installing Old Templates

If you had previously downloaded and installed files which had the names "AMSAgent.admx" and "AMSAgent.adml", these should be removed. Do so as follows:

- To un-install from a single machine:
  1. Delete AMSAgent.admx from `%systemroot%\PolicyDefinitions`
  2. Delete AMSAgent.adml from `%systemroot%\PolicyDefinitions\en-US`
- To un-install from a Domain Controller:

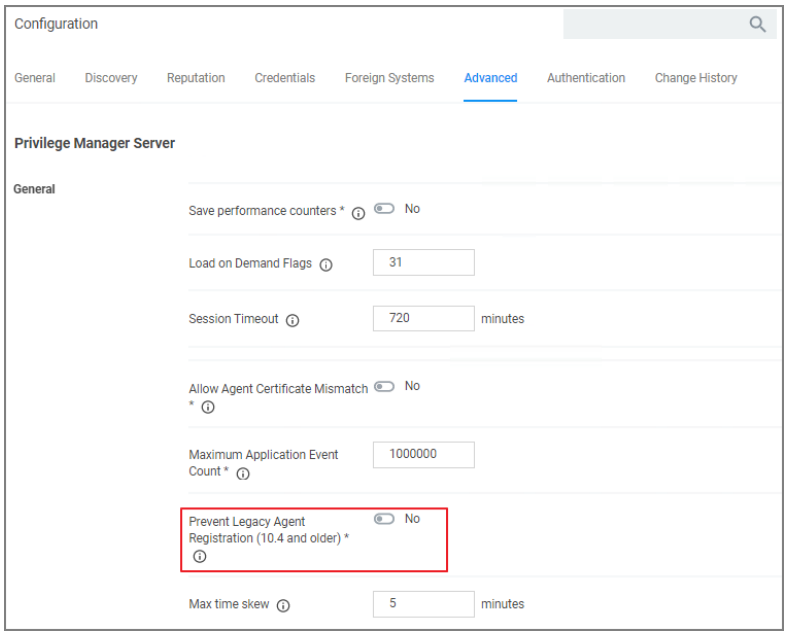
1. Delete AMSAgent.admx from `%systemroot%\SYSVOL\domain\Policies\PolicyDefinitions`
2. Delete AMSAgent.adml from `%systemroot%\SYSVOL\domain\Policies\PolicyDefinitions\en-US`

How to prevent Backwards Compatibility for Agents v10.4 and earlier

Starting in Privilege Manager version 10.5 and up, due to security updates you can now prevent services from using agents versions 10.4 and earlier from communicating with the Privilege Manager server.

Resolve

1. Launch Privilege Manager.
2. Navigate to **Admin** | **Configuration**.
3. Click the **Advanced** tab.
4. Set the **Prevent Legacy Agent Registration (10.4 and older)** to **Yes**.



5. Click **Save Changes**.

VM Deployments

Privilege Manager agents are installed on endpoint machines to implement policies which are defined by the user (the Privilege Manager administrator) in the Privilege Manager console (the user interface of the Privilege Manager Server).

This article is about agent deployment to endpoints in Virtual Desktop Infrastructure (VDI) or other similar environments. It describes the different cases and options for deploying Privilege Manager agents to VDIs and discusses the pros and cons where relevant. It is expected to be read by a user who is the Privilege Manager administrator for the customer.

Installing the Privilege Manager agent is supported as part of a VDI image build. There are a few different ways to accomplish this, based on the (Privilege Manager) customer's environment and preferences. Discussion of the relevant issues and options is grouped in this article as follows:

Identifying Agents to The Console

The pertinent question here is: Do you (the user) plan to use (or are using) persistent virtual machines (VMs) or dynamic VMs? There are different implications for each of these, discussed below.

Persistent VMs

In a persistent VM, machines images are created, spun up, and then persist indefinitely. This case is fairly simple. We can treat these machines the same as we would physical machines except for concerns around the universally unique identifier (UUID), which will be discussed further on (in the section, “Multiple VMs Collapsed to a Single Resource”).

Dynamic VMs

In a dynamic VM, a golden image is spun up each time a user requests it with their profile and it is then applied on top. This case is more complicated.

The major concern is agent spamming, which would happen as follows: the Privilege Manager console sees each new image as a new computer and rapidly runs through the customer's licenses, leaving a large number of orphan machines. There are a few different ways to deal with this situation, discussed in the sub-sections below.

Multiple VMs Collapsed to a Single Resource

The easiest way to support dynamic VMs is for you to collapse all of your VMs to a single computer resource on the console. This can be accomplished as follows:

1. Add a registry entry in HKLM\Software\Arellia\Agent called “AgentIdOverride.”
2. Install the agent on a physical computer and allow it to register.
3. Next, in the Privilege Manager console:
   a. Navigate to Admin > Agents.
   b. Click on one of the charts to view a list of registered computers.
   c. Find the computer in the report and click on it. This will take you to the Resource View of that computer. The ID for this computer is the UUID displayed as the last part of the URL (after “/item/view/”) in the browser address bar.
   d. Copy this ID value (the last part of the browser URL).
4. Place the copied ID value in the AgendIdOverride registry entry.

Alternatively, if you want multiple VDI images to which differing policy sets are applied, you could have different values. The rollup computers in the console could then be assigned to the appropriate resource targets.

The benefits of this approach are:

- It is by far the simplest to implement.
- It results in the fewest licensing issues.

- Moreover, because the resources are created ahead of time they can be inventoried and assigned to the appropriate resource targets. Consequently, a machine would get the appropriate policies as soon as it spins up with no need to wait for processes to run either on the desktop or server.

The downside of this approach is:

- There would be some loss of fidelity in data on the console, specifically around which machine an event happened on. However, since virtual desktops are by nature transitory that may be less of a concern. Privilege Manager will still attach usernames to the event data so you will know “who” (the end user) if not necessarily “where” (the specific endpoint).

Pool of Values to Support Multiple VMs

If you wish to be more specific, the following technique could be used: create a pool of UUID values to be assigned to the AgentIDOverride and assign one from this pool when the machine spins up.

With this technique, as part of the VDI provisioning, Privilege Manager would trigger the basic inventory task to make sure that the server gets correct information on the machine name and details. You would want a pool of values rather than a random one to prevent spamming new agents. Reusing the values would keep that under control.

Managing Agent Trust and Certificates

This section discusses certificate management.

As of version 10.5, Privilege Manager validates agent certificates against the specific agent that was initially registered. There are two cases:

- All desktops using a single agentID: This case is fairly straightforward. A single certificate would be included as part of the desktop image which would match what was stored in the database for that ID and all of the communication would be accepted.
- A pool of IDs: In this case, there are two potential ways to do certificate management:
  - Method 1: Navigate to Admin > Configuration > Advanced; select the "Allow Agent Certificate Mismatch" option; turn on the option. (It is off by default.)
  - Method 2: Deploy the install code on machine imaging, as follows:
    - Add a registry entry in HKLM\Software\Arellia\Agent of type String and call it “InstallCode.”
    - In the Privilege Manager console:
      - Navigate to Admin > Agents > “Installation Codes” tab.
      - Click “Copy” to copy the value displayed under Code.
    - Paste the copied value into the InstallCode registry entry.
    - Once this entry is set, then during the agent registration process, the agent sends this InstallCode up to the server along with whatever certificate it has. This overrides the database entry and allows that agent to communicate as long as it is up and running.

Minimizing Time Between VDI Deployment and Policy Enforcement

This section is about policy deployment.

In a non-VDI environment, when Privilege Manager deploys agents to desktops, there can be a significant delay between deployment and policy enforcement and it is not a concern because it is a one-time issue.

However, in the case of VDI, machines are created and recreated daily and this delay becomes a larger issue. In this case, you must make sure that the Client Items database, with the appropriate policies, is part of the initial desktop image. This file can be created in C:\ProgramData\Arellia\ClientItems and can be simply copied from a machine that has the agent deployed and all policies downloaded.

However, if any policy changes are made after image creation you would need to either update that file in the golden image or add a post-deployment step to run the Powershell script “C:\Program Files\Thycotic\Powershell\Arellia.Agent\UpdateClientItems.ps1” and trigger the virtual desktop to download the latest policy items.

Licensing Concerns with Windows 10 Amazon Workspaces

This section discusses licensing concerns, specifically with Windows 10 Amazon Workspaces.

Although Amazon claims to offer a Windows 10 VDI environment, what they offer is not technically speaking Windows 10. Rather, what they provide is a Windows Server 2016 environment running what they call Windows 10 Experience.

This means that when Privilege Manager inventories it, the Privilege Manger agent believes that it is running on a server class OS. Therefore, from a licensing perspective, Amazon Workspaces need to be licensed as servers, rather than as clients.

Agents on macOS Systems

This section of the Privilege Manager documentation covers information and step procedures pertaining to Privilege Manager agents installed on macOS.

The following topics are available:

- Agent Configuration
- Agent Hardening
- Modify Update Agent Commands (macOS) Policy
- macOS Agent Utility Preference Pane
- Terminal Commands
- Finding Logs without using the Agent Utility
- Using an MDM Profile for your Agent
- Troubleshooting

macOS Agent Hardening

It is not currently possible to prevent a local administrator account on macOS from starting and stopping a background service like the Privilege Manager agent. The generally accepted best practice is for the end user to log into a "standard" (non-administrative) account. This should not be a hardship in conjunction with Privilege Manager, once an appropriate but limited set of tools are enabled for the end user.

When the Privilege Manager agent is installed on a macOS endpoint, three processes run in the background. Two of these are macOS launch daemons that run as root, and the third is a macOS launch agent that runs in the current user's context. These processes are run by the `launchd` process, which will automatically relaunch them if they are terminated. Moving Privilege Manager to the Trash in an attempt to disable the functionality will not be allowed by the Finder while the processes are still running; bypassing this requires administrative privileges.

Note: The term "launch agent" has a specific meaning in macOS, and is not related to the use of the word "agent" to describe the Privilege Manager endpoint software.

In addition, a sudo plugin is installed that connects the `sudo` command to the Privilege Manager policy engine. This modifies the default behavior of the `sudo` command.

Possible Areas of Concern

- An administrative user could use the `launchctl` command to disable the Privilege Manager processes (the launch daemons `com.delinea.acsd` and `pmcored` and the launch agent Privilege Manager).

  To mitigate, create a blocking policy for `/bin/launchctl`. "Creating a File Specification Filter" on page 344 prevents a privileged user from unloading, removing, and/or stopping either of the above LaunchDaemons and LaunchAgents.
- The application bundle `Privilege Manager.app` could be deleted from the command line by an administrative user (possibly after first disabling the sudo plugin).
- The sudo plugin could be disabled by an administrative user by removing or renaming the file `/etc/sudo.conf`. This can be done from the Finder (i.e., even if the normal use of sudo is blocked by policies implemented through the plugin itself, or if the plugin fails to work normally due to other issues with Privilege Manager).
- On most Unix systems, the command `su` can be used to log into the root account (assuming one knows the root password), which gives complete access to the system. On macOS the root account is disabled by default, but can be enabled by an administrative user; see the Apple support document at https://support.apple.com/en-us/HT204012.

Refer to this video demonstration.

Locations of Privilege Manager Files

The Privilege Manager agent is implemented by files in the following locations:

- `/Applications/Privilege Manager.app`

  This application bundle contains the Privilege Manager launch agent and the `com.delinea.acsd` launch daemon, which together implement the main functionality of the PM agent.
- `/Library/Application Support/Delinea/Agent`

  This folder contains background items, configuration information, and other data necessary for the Privilege Manager agent.
- `/Library/LaunchAgents/com.delinea.acsgui.plist`

  This file is used by the macOS launchd system service to start the Privilege Manager launch agent when the user logs in.
- `/Library/LaunchDaemons`

Privilege Manager installs a number of plist files into this folder; the macOS launchd system service uses these files to start the Privilege Manager background processes when the Mac starts up or as required.

- `/Library/SystemExtensions`

  In macOS Big Sur and later, the `com.delinea.acsd.systemextension` system extension is automatically copied into this folder when Privilege Manager is first installed. If Privilege Manager is uninstalled, the extension will be deactivated by the system and will be fully removed when the Mac is next restarted. This is currently only possible if SIP is disabled.

- `/usr/local/delinea/agent`

  This folder contains a number of shell scripts that are present for compatibility with older versions of the Privilege Manager agent (they now invoke the `pmagentctl` command line tool).

- `/usr/local/libexec/sudo`

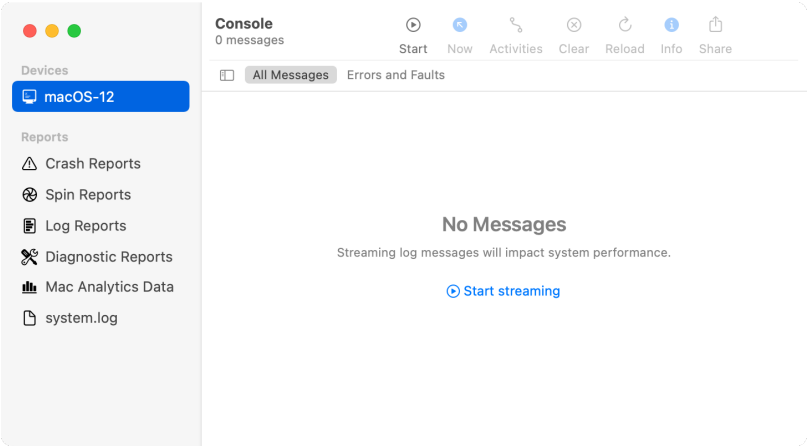
  This folder contains the sudo plugin `delinea_plugin.so` that integrates Privilege Manager with the sudo command.

- `/etc/sudo.conf`

  This file is added by the Privilege Manager installer to configure the `sudo` command to use the Delinea sudo plugin `delinea_plugin.so` when it is run from the command line.

Finding Logs for Troubleshooting

For troubleshooting your macOS agent, logs are found in the macOS Console application.



In the left menu from your macOS Console application, select your computer under **Devices**, then select **Start streaming** to view logs.

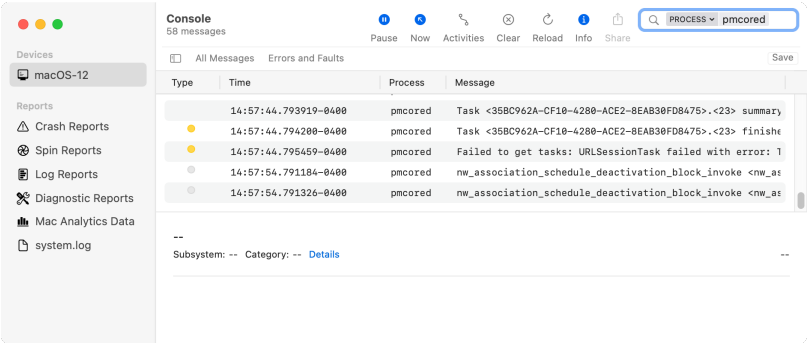
In the Console **Action** tab, choose to include information, debug messages, or both.

There are certain processes you can filter on to troubleshoot the agent. They are:

- pmcored
- pmeventuploaderd
- pmeventprocessord

- pmfileinventoryd
- pmlocalsecurityd

This is an example of filtering on the process "pmcored."



Using MDM Profiles for your Agent

If you utilize an MDM solution, you can create configuration profiles to make management of the agent silent on macOS deployments. We recommend deploying the relevant SYSEX or KEXT profiles prior to the agent deployment.

It is recommended to use the System Extension version, as Apple has deprecated the use of Kernel Extensions. Refer to Software Downloads/macOS Endpoints

System Extension (SYSEX)

System Extension Allow Payload

Inside your MDM, create a System Extension Allow profile based on the below information:

- Team Identifier: UJDHBB2D6Q
- Allowed System Extensions: com.thycotic.acsd

SYSEX Privacy Preferences Policy Control (PPPC) Full Disk Access Payload

Inside your MDM, create a PPPC profile based on below:

- Identifier: com.thycotic.acsd
- Identifier Type: Bundle ID
- Code Requirement:

```
anchor apple generic and identifier "com.thycotic.acsd" and (certificate leaf
[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1
[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf
[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
UJDHBB2D6Q)
```

- Service and Key Value: SystemPolicyAllFiles: Allow

(PPPC) Allow Notifications Payload

Refer to: Manage Privilege Manager Notifications on macOS

(PPPC) Allow AppleEvents and Accessibility Payload

Refer to the bottom of the page: "Application Approval Request Message Action" on page 338.

Kernel Extension (KEXT)

Apple has deprecated the use of Kernel Extensions. The KEXT version is still available but macOS version dependent. Refer to Software Downloads: macOS Endpoints

Kernel Extension Allow Payload

Inside your MDM, create a Kernel Extension Allow profile based on the below information:

- Team ID: UJDHBB2D6Q
- Kernel Extension Bundle ID: com.thycotic.ThycoticACS

KEXT Privacy Preferences Policy Control (PPPC) Full Disk Access Payload

Inside your MDM, create a PPPC profile based on below:

- Identifier: com.thycotic.ThycoticACS
- Identifier Type: Bundle ID
- Code Requirement:

```
anchor apple generic and identifier "com.thycotic.ThycoticACS" and (certificate leaf
[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1
[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf
[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
UJDHBB2D6Q)
```

- Service and Key Value: SystemPolicyAllFiles: Allow

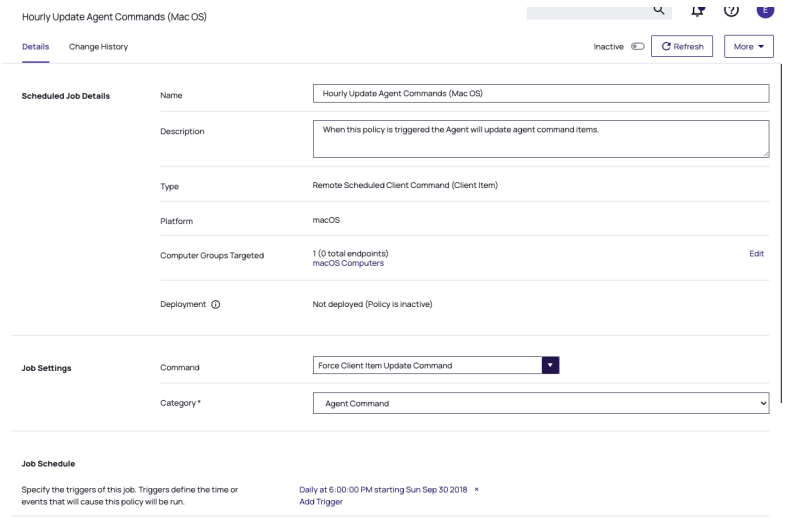
Modify Update Agent Commands (macOS) Policy

Agents receive new policies on a schedule which can be modified. By default this schedule runs daily at 8 pm.

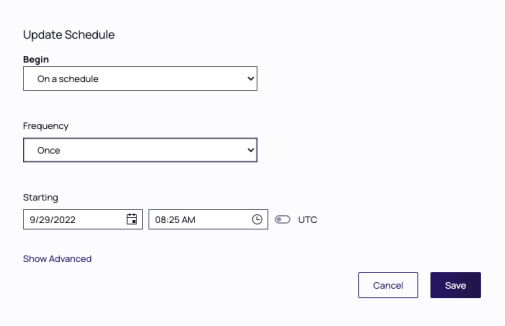
To create a modified schedule, you have to duplicate the default Scheduled Job and customize the duplicate:

1. Under your macOS computer group, select **Scheduled Jobs**.
2. Search for and select **Update Agent Commands (macOS)**.
3. Click **Duplicate**.

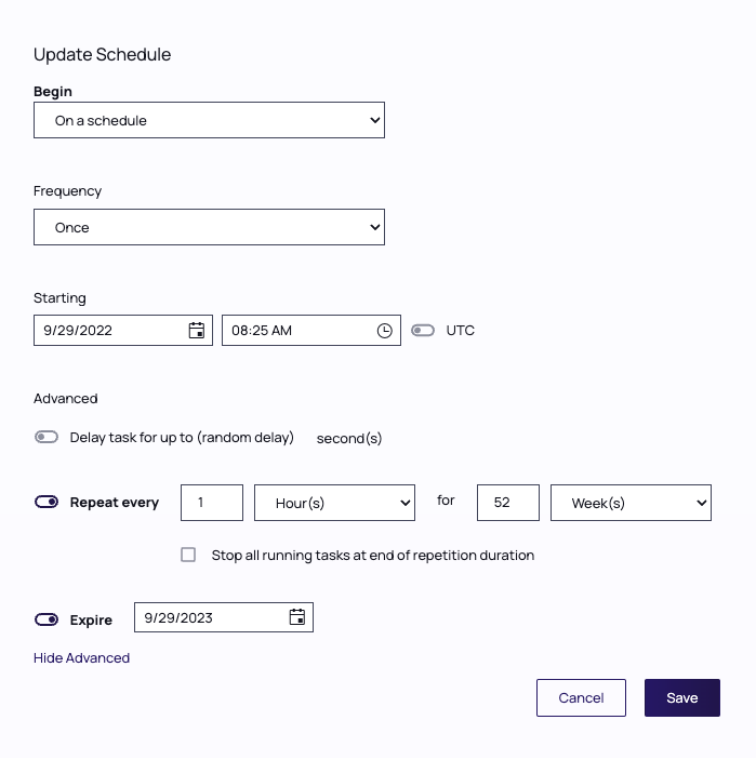
4. Enter a name for this duplicated task that reflects its purpose. For example, if it is supposed to run hourly, reflect it in the name.
5. Click **Create**.



6. Under the Job Schedule section,
   a. Click on the **x** to remove the *Daily at 8:00:00 PM ...* schedule.
   b. Click **Add Trigger**.

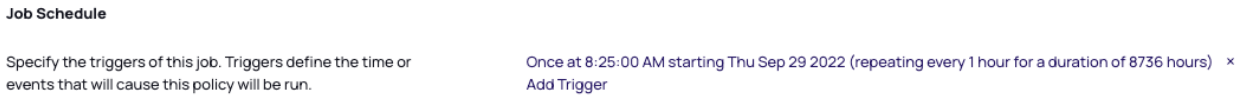


   c. For the **Begin** drop-down, keep the **On a schedule** selection.
   d. Maintain the **Once** selection at the **Frequency** drop-down.
   e. Click **Advanced**.
   f. Make the changes to run the task hourly and specify for how long. For this example we selected to run this task hourly for 52 weeks with an expiration date of one year from the starting date. Setting an expiration date is not required.



g. Click **Save**.

7. Click **Save Changes**.



Terminal Commands

In the macOS Terminal application you can perform the following commands directly to your Delinea macOS agent, using the pmagentctl utility.

To find this list, enter the following into Terminal:

pmagentctl

Commands returned for the pmagentctl Utility

Overview: PM Agent Control

Usage: pmagentctl < *subcommand* >

Options:

--version (show the version)

-h, --help (show help information)

Subcommands

subcommand	description
agentid	Gets the Agent ID
dumpconfig	Gets Agent Configuration Data
register	Initiates an Agent registration (requires elevated privileges)
server	Set server URL and optional install code (requires elevated privileges)
isregistered	Gets the Agent registration status
updateclientitems	Update client items (requires elevated privileges)
listclientitems	List client items. By default, all categories of client items are included
runschedule	Policy ID to run (requires elevated privileges)
sendevents	Sends events (requires elevated privileges)
start	Starts the agent (requires elevated privileges)
stop	Stops the agent (requires elevated privileges)
restart	Restarts the agent (requires elevated privileges)

See pmagentctl help < *subcommand* > for detailed help.

Command Usage

To perform a command, insert the name of the above command that you need to perform into this command string:

pmagentctl < *InsertCommandHere* >

Note: The start, stop, and restart commands are required to be run via sudo. This will prompt for admin account password verification. The other commands that require elevated privileges can be run via sudo or credentials can be entered interactively.

For example, to register an agent immediately after updating the Privilege Manager server location, type:

sudo pmagentctl register

Legacy Path and Scripts

Previously, you would use the utility with a path like:

sudo /usr/local/thycotic/agent/agentUtil.sh < *InsertCommandHere* >

The legacy scripts are still available and can be used, but they are now located in:

/usr/local/delinea/

The /usr/local/thycotic/ directory is a symlink to the /usr/local/ delinea/ directory.

These legacy scripts are deprecated and will be removed in future releases, so using the pmagentctl utility when possible is recommended.

macOS Agent Utility Preference Pane

With the 10.8 release of Privilege Manager, Delinea introduced a UI based macOS Agent Utility implemented as a preference pane. The utility provides functionality previously only available via Terminal shell commands. The utility allows customers to easily troubleshoot by

- checking an endpoint status.
- view an endpoint cache.

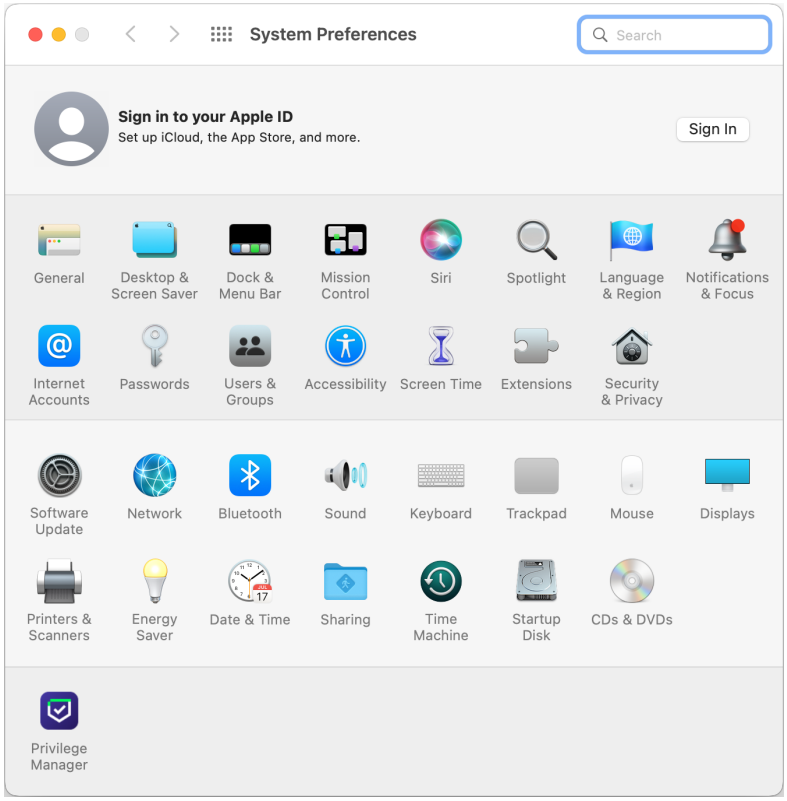
It also offers UI guided means to

- register the agent with the server.
- update the endpoint to retrieve latest policies.

Accessing the Agent Utility

To access the Privilege ManagermacOS Agent Utility,

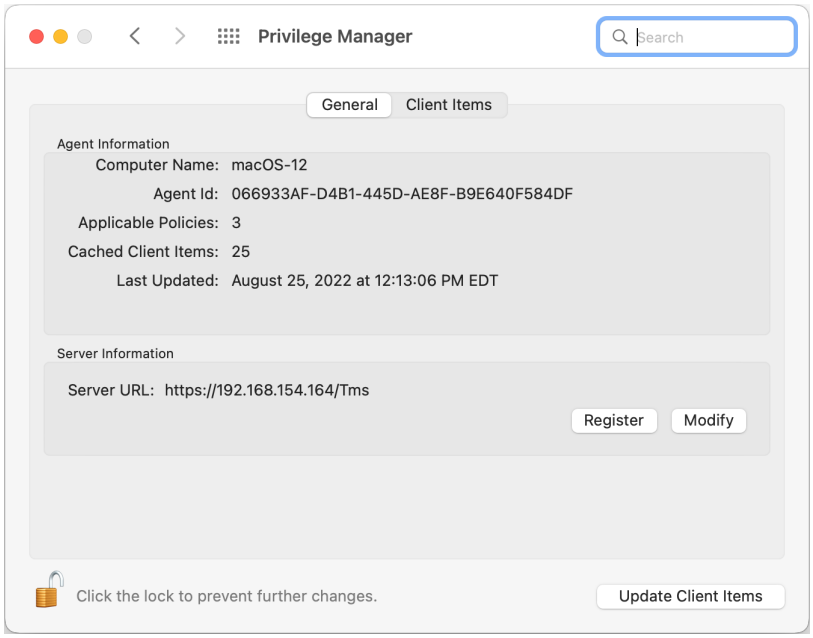
1. Open the System Preferences on your macOS endpoint.



2. Click **Privilege Manager** to open the preference pane.

General Tab

When a local admin user opens the utility, the controls to make changes are unlocked. For standard users they are locked, but can be unlocked by providing an administrator user name and password, just as possible with all other preference panes.



On the general tab the utility provides under **Agent Information** details like the Computer Name, Agent Id, the number of applicable policies and client items cached. It also provides the data/time stamp of the last update.

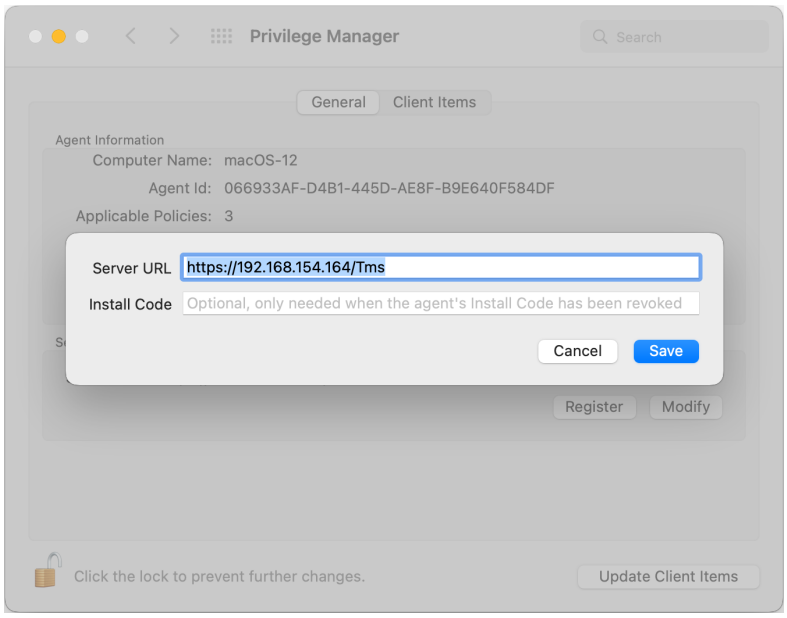
Under **Server Information** the Server URL for the current agent registration is listed. Here, administrator users can either Register a not yet registered agent, or modify an existing agent registration.

Use **Update Client Items** to trigger a client item update. When **Update Client Items** is clicked and if there are updates to applicable policies or policies are added to the endpoint, the last updated timestamp will change to reflect when the last client items change on the endpoint happened. The date/time stamp does not reflect when the last update client items command ran, the date/time stamp only updates when there was an actual change on the endpoint.

Registering/Modifying an Agent

To register an agent or to modify an existing agent registration via agent utility, follow these steps:

1. Open the Privilege Manageragent utility.
2. On the General tab under Server Information click Register or Modify.



a. Enter the **Server URL** for the agent registration or modified registration.

b. If the agent has been installed without an install code or the agent's registration was revoked, provide an install code to register the agent.

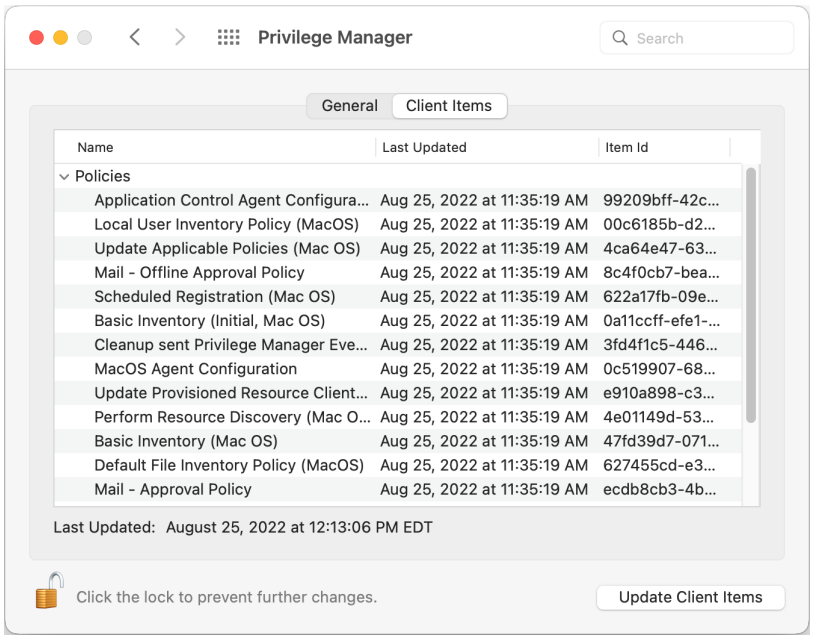
c. Click **Save**.

Client Items Tab

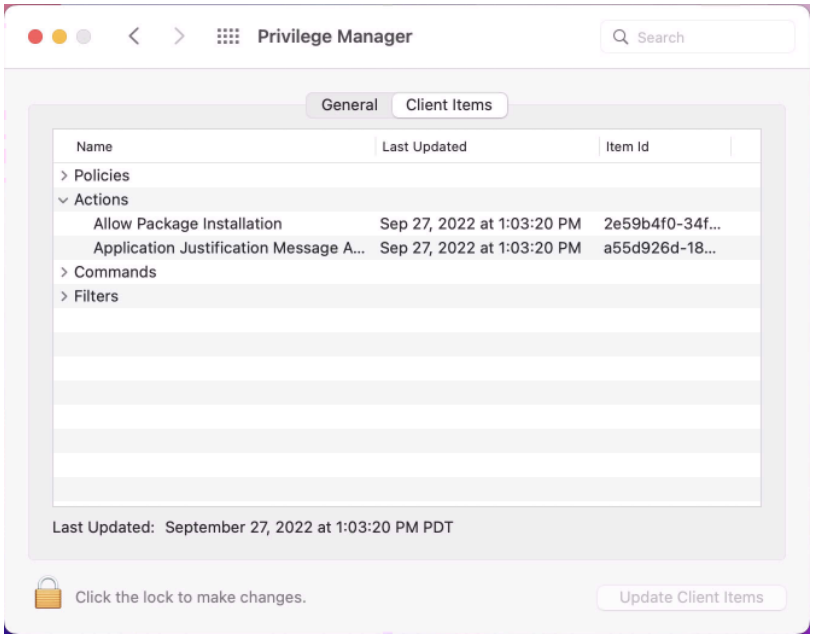
The Client Items tab provides an overview of all client items on the endpoint. The client items are grouped into the following categories:

- Policies
- Actions
- Commands
- Filters
- Provisioned Resources

The following image shows the client items on the endpoint in an unlocked preference pane with policies expanded.

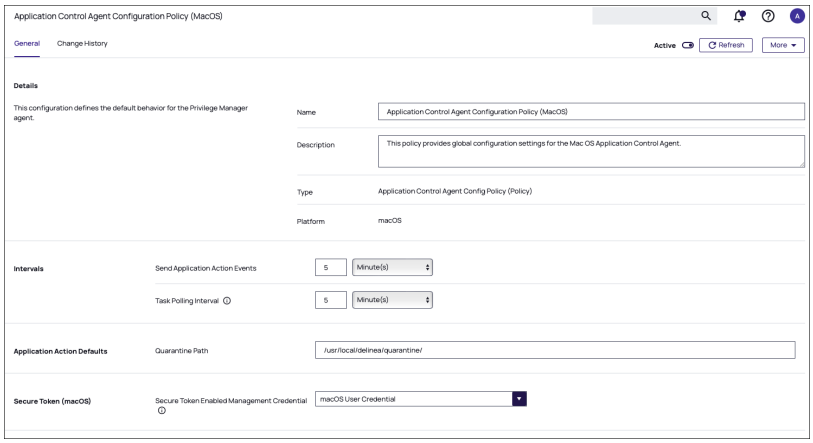


Use expand/collapse to better navigate through the list of applicable client items on the endpoint. The following image shows the client items on the endpoint in a locked preference pane with policies, commands, filters, and provisioned resources collapsed.



Agent Configuration

Under each macOS Computer Group, administrators can specify global application control agent settings for the specific Computer Group.



- Details: This section contains the policy details such as name, description, and platform information.
- Self-Elevation: This section provides a configuration option to enable the Allow Self-Elevation option.

  Note: Self-Elevation is deprecated and only supported on macOS v10.8 or earlier.

  An application policy will need to be enabled to define what action is applied when a user requests an elevation. The menu text can be customized via the Menu Text field.

  - Default: Request run as administrator
- Intervals: This section provides a configuration option to customize the intervals at which the agent will send application action events or how often a macOS Agent will callback to the server to see if any tasks have been requested of it.
  - Defaults:
    - Send Application Action Events: 5 Minutes
    - Task Polling Interval: 1 Minute
- Application Action Defaults: This section provides the option to set the quarantine path.
  - Defaults:
    - Quarantine Path: /usr/local/delinea/quarantine/
- Secure Token (macOS): This section provides an option to specify a macOS admin account that is Secure Token enabled. This account must exist on all LSS managed macOS endpoints.

Troubleshooting on macOS Workstations

The following topics offer troubleshooting help for macOS workstations and agents:

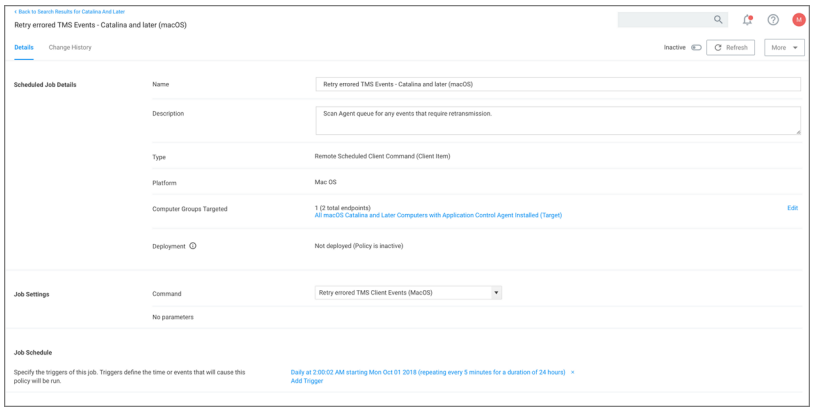
- macOS - FileSystemWatcher
- How to Recover an Unresponsive macOS Endpoint
- Sudo Command Timed Out

Catalina FileSystemWatcher Issue

Note: This policy is only applicable with agents prior to Privilege Manager v11.2.0.

There is a known issue on macOS Catalina and later versions, preventing the agent from receiving notification of events that need to be sent to the server. To workaround this, the **Retry errored TMS Events - Catalina and later (macOS)** policy can be enabled to ensure all events get sent to the server.

The defaults for this new Remote Scheduled Client Command are as follows:



- Customize the schedule if necessary to best suit your particular implementation.
- The default resource targets required are specified by default as **All macOS Catalina and later Computers with Application Control Agent Installed (Target)**. The results of the computer group include any macOS Catalina computers that have the agent installed and are properly configured for Application Control.

Once the policy is enabled on an endpoint, the agent will perform the **Retry errored TMS Client Events (macOS)** command and send any events that have not been sent.

How to Recover an Unresponsive macOS Workstation

In case a macOS workstation ever becomes unresponsive due to conflicting policy configurations, the following steps allow a user to recover the workstation without having to restore or rebuild the system.

Note: Applies to all macOS versions on which the KEXT is supported.

1. Turn off the macOS system.
2. Hold down the ⌘ +s keys and power the system back on. Keep holding those keys down until it shows that it is booting in single-user mode.
3. Follow the prompts to mount the root device as read-write. It will instruct you to enter the following:

```
/sbin/fsck -fy
/sbin/mount -uw /
```

4. Rename the kernel extension so that you can get back to a functioning macOS:

```
cd /Library/Extensions
mv ThycoticACS.kext ThycoticACS.kext.orgexit
```

5. The system will restart.
6. Disable and/or delete policies that are causing the issue.
7. Update client items before renaming the kernel extension and having it start automatically. You can force client item updates by performing the following in Terminal.app:

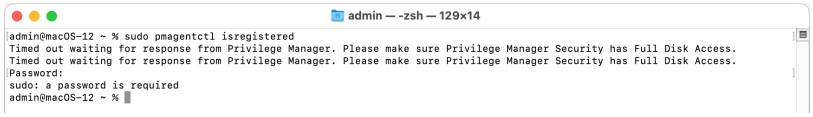
```
sudo /usr/local/delinea/agent/updateClientItems.sh
```

8. Restore the kernel extension in Terminal.app:

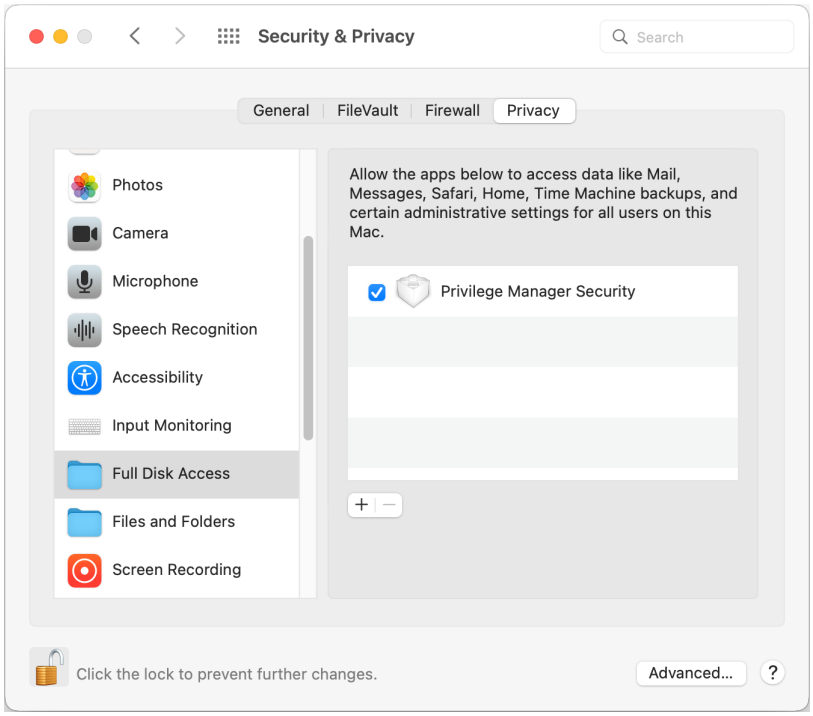
```
cd /Library/Extensions
sudo mv ThycoticACS.kext.org ThycoticACS.kextexit
```

Sudo Command Timed Out

The sudo plugin, which allows you to run commands elevated via the terminal, can experience a time out if the Privilege Manageragent hasn't been granted Full Disk Access. When the agent hasn't been granted Full Disk Access, you may see an error similar to:



To grant Full Disk Access to the Privilege Manager agent manually, go to **System Preferences > Security & Privacy > Privacy > Full Disk Access** and check the box next to **Privilege Manager Security.**



To grant Full Disk Access to the Privilege Manager agent via an MDM Profile, follow the instructions outlined here

After the agent is given Full Disk Access, `sudo` commands should begin to evaluate successfully.

Agents on Windows Systems

This section of the Privilege Manager documentation covers information and step procedures pertaining to Privilege Manager agents installed on Windows systems.

The following topics are available:

- Agent Configuration
- Windows Agent Utility
- Agent Hardening 10.7.1 and up
- Pre-10.7.1 Agent Hardening
- Setting the Server Address
- Elevating Fully Trusted Universal Windows Platform (UWP) Applications
- Troubleshooting
- Memory Protection

Agent Hardening 10.7.1 and up

Agent installations on endpoints can be secured, only allowing a specified user access to start or stop an agent service and denying any agent control access to a local Administrator or basic user account.

To make sure that local Administrators do not tamper with Delinea agents running on their system, Privilege Manager Administrators can define users that can start and stop the Privilege Manager services running on endpoints, such as the Delinea Agent or Delinea Application Control.

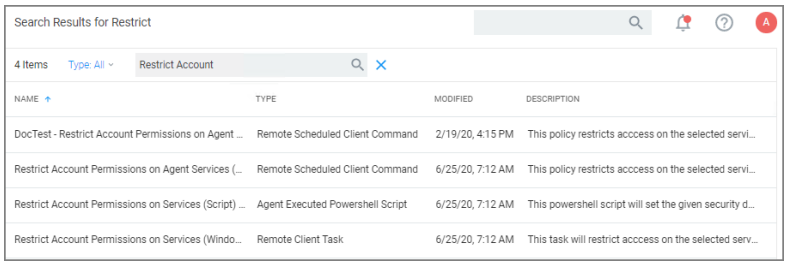
A user or group needs to be available in Privilege Manager to be selected while setting up the task. This user or group will have rights to start and stop agent services running on endpoints once the **Restrict Account Permissions on Agent Services (Windows)** policy is enabled.

Note: If you implemented Agent Hardening prior to 10.7.1, **disable** and **delete** the following policies:

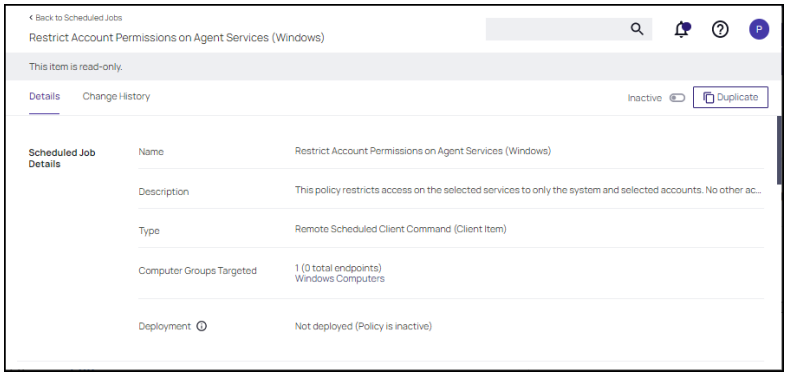
- Agent Service Start / Stop Control (Windows)
- Agent Service Clear Restrictions (Windows)

Editing the Restrict Account Permissions on Agent Services (Windows) Policy

1. Under your Computer Group, select **Scheduled Jobs**.
2. Search for **Restrict Account**.

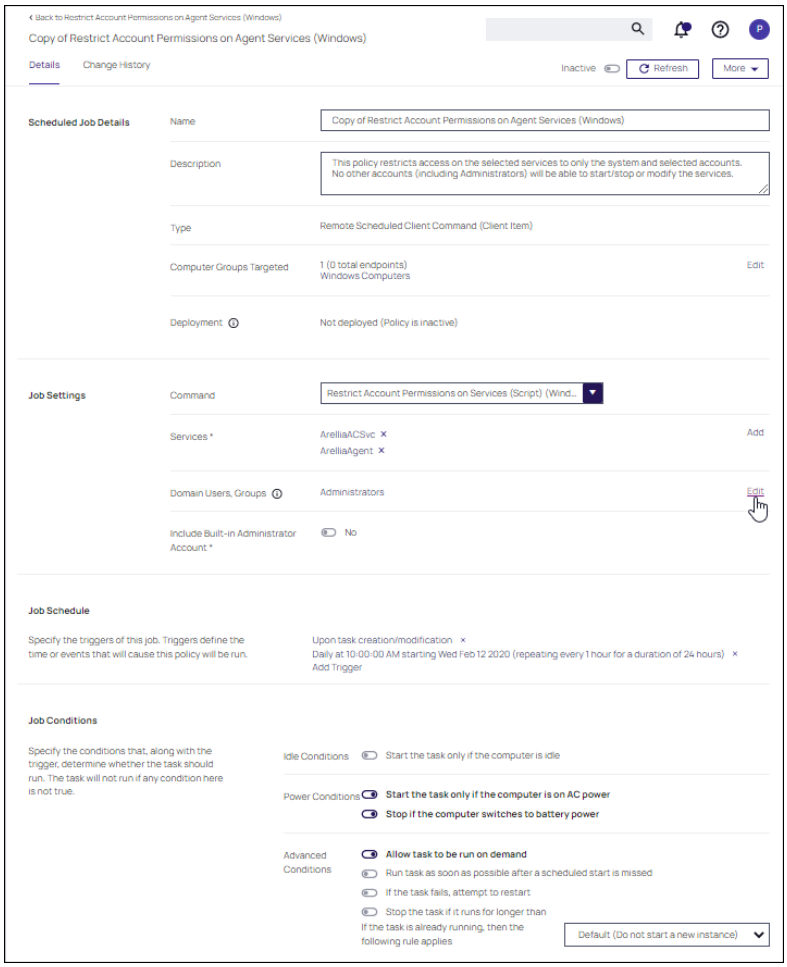


3. Click on the **Restrict Account Permissions on Agent Services (Windows)** policy. To customize the policy click **Duplicate**.



4. Customize the name of the copied policy and click **Create**.

5. Customize the policy's **Scheduled Job Details**, **Job Settings**, **Job Schedule**, and **Job Conditions**.
   a. Under **Services** the Arellia Application Control Service and Arellia Agent Service are present by default. Add any services you might also want to protect. Use the search field to find and specify other service names.
   b. For **Domain Users, Groups** use **Edit** and use the search field to find specific user accounts that have permissions to make changes to the specified services. Administrators are present by default, if you wish to limit to only a subset of users with administrative rights, create a group and update accordingly.
   c. Use the **Include Built-In Administrator Account** toggle to determine whether to include the built-in administrator.
6. Click **Save Changes**.



7. Set the policy to **Active**.

> **Note:** If you wish to update a hardened agent, refer to information under the topic Windows Agents | Hardened Agents.

Setting the Privilege Manager Server Address

Agents require a Privilege Manager Server to communicate with. The recommended way to set the URL address is during the installation of the Delinea Agent. If an Azure Service Bus or Reverse Proxy is used, the URL can point at the URL of those components.

The URL address can be changed post-install via the registry or PowerShell.

Setting the Privilege Manager Server (TMS) Address via PowerShell

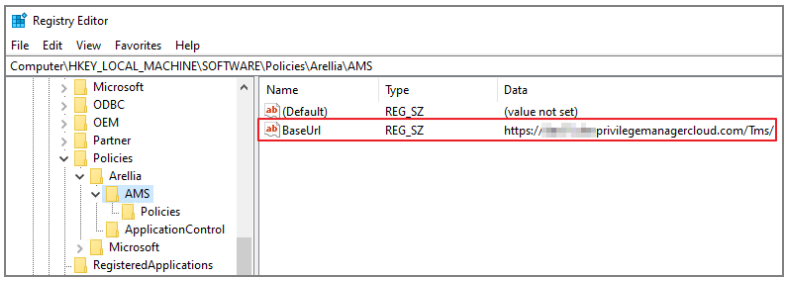
To set the Privilege Manager Server (TMS) address via PowerShell, run this command as Administrator:

```
C:\Program Files\Thycotic\Powershell\Arellia.Agent\SetAmsServer.ps1
```

The script will then ask you to type in the fully qualified domain name of the server.

Changing the Privilege Manager Server (TMS) Address via the Registry Editor

1. Open the Registry Editor (regedit)
2. Navigate to **HKEY_LOCAL_MACHINE | SOFTWARE | Policies | Arellia | AMS**.
3. Right click BaseUrl and select Modify.



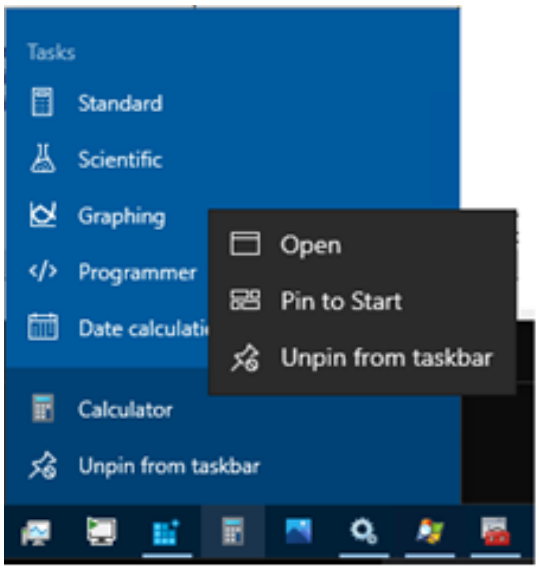
4. In the Edit String dialog box, change the BaseURL to your TMS Address.
5. Close the registry.
6. Restart the Agent service.

Elevation Support for Fully-Trusted UWP Apps

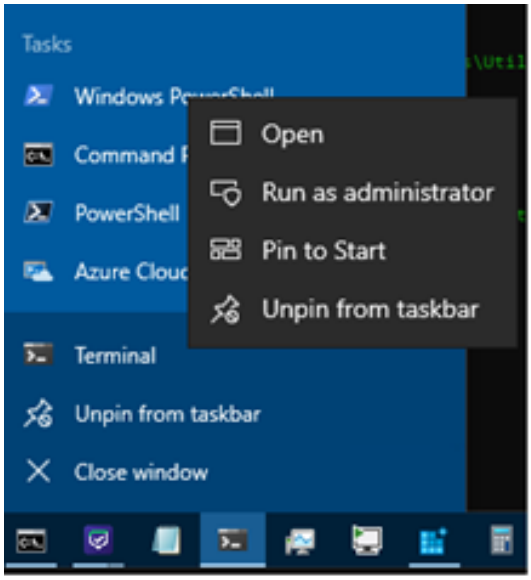
Universal Windows Platform (UWP) apps, also known as Windows Store apps, Modern apps, Immersive apps or UAP Universal Application Platform (UAP) apps, all refer to the same thing. UWP apps are obtained from the Windows Store, although some are pre-installed on Windows 10/11. These apps exist in a couple of different varieties, with two of them being the most frequently encountered.

The first type is the basic Windows Store application, which cannot be elevated. They are limited to using just the WinRT [Windows RunTime] API library and lack access to the Win32 API library. The Calculator app on Windows 10 and newer is a good example of a basic Windows Store app.

The easiest way to identify an app of this type is to find the pinned item for it on the modern Start menu or task bar, right-click and select **Calculator**. Note that **Open** is present but **Run as administrator** is not present. The lack of an option to run the app as an administrator indicates that the app cannot be run elevated.



The second type is the fully-trusted UWP app. These apps are also known as Centennial Desktop Bridge apps. Although they utilize the WinRT API library in order to use the modern UI styling, they also have full access to the Win32 API and are capable of being run elevated. As with basic apps, a fully-trusted UWP app can be identified by its pinned item on the modern Start menu or task bar Right-click, select the app and observe that both **Open** and **Run as administrator** are present. The presence **Run as administrator** indicates that the app can be run elevated and the PrivMan Agent for Windows 11.4.0 and newer, and you can apply an elevation policy to instances of the fully-trusted UWP app.



Well-known fully-trusted UWP apps include WindowsTerminal on Windows 10 and newer, and Notepad on Windows 11, now a fully-trusted UWP app rather than a Win32 Desktop application.

There are additional types of UWP apps that fall somewhere in between basic and fully-trusted. Only Microsoft can publish a UWP app that is manifested and flagged as being fully-trusted. Fully-trusted UWP apps are also known as Inbox apps, rather than Windows Store apps. Certain third-party apps may also have programs that are intended to

run elevated, but they are identified differently from how an Inbox fully-trusted UWP app published by Microsoft would be identified.

The “somewhere in between” category of UWP apps has primarily to do with an app package being installed that consists of multiple application programs, where the primary app in the package is a Basic Store app that cannot run elevated. However, there are also one or more application programs present in the package which can be run elevated. In this case, with these being third-party apps made available via the Windows Store, the package has the `runFullTrust` capability listed in the overall package manifest and then the per-application manifest for specific programs in the package will also contain the `runFullTrust` capability. Currently, the 11.4.0 version of the PrivMan Agent for Windows does not support elevating `runFullTrust` third-party UWP apps. Support for doing so will be added in a future release.

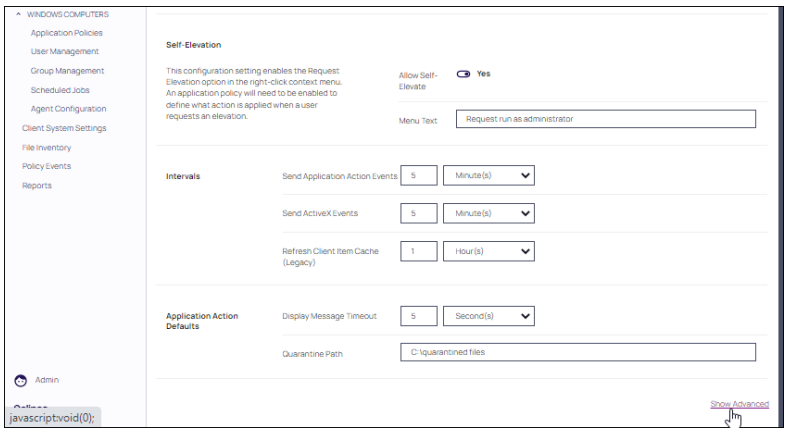
Please note that UWP apps must be installed on a per-user basis. Even though the Windows Trusted Installer will allow a non-privileged user to install a UWP application package, and the program files and related collateral will be located in a folder nested under C:\Program Files\WindowsApps, there are still some per-user installation tasks that get performed to make the app available in the user’s profile on that particular computer. Our agent does not check for, nor does it perform this per-user registration of UWP apps. However, if it detects that a fully-trusted UWP app has been launched, the agent will attempt to apply policies to it.

Memory Protection for Windows Agent Hardening 10.7.1 and Higher

For Agents running Windows, you may need to check the status of the **Memory protection enabled** setting.

Note: As indicated by the Warning, you should seek the assistance of support personnel to determine the correct setting of this control.

1. To access this control, open Windows Computers in the left navigation panel and select **Agent Configuration**.
2. At the bottom of the page, click **Advanced Settings**.

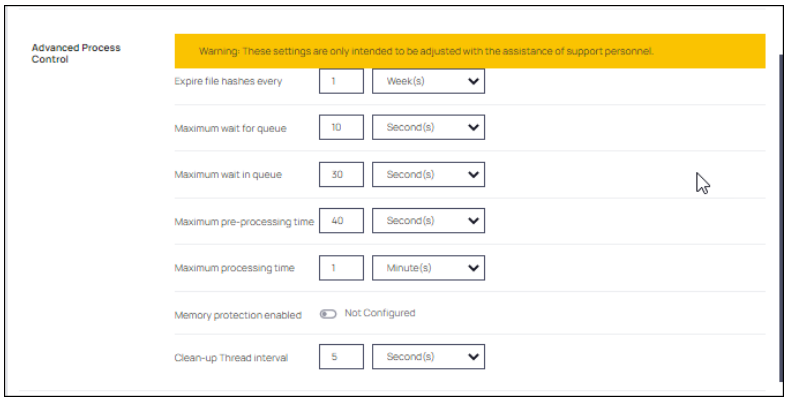


3. Locate the **Memory protection enabled** toggle in the **Advanced Process Control** section.

   By default, this control is not configured and remains in an enabled state.

   In most cases, disable the toggle if your system has memory protection enabled in your anti-virus protection

software.

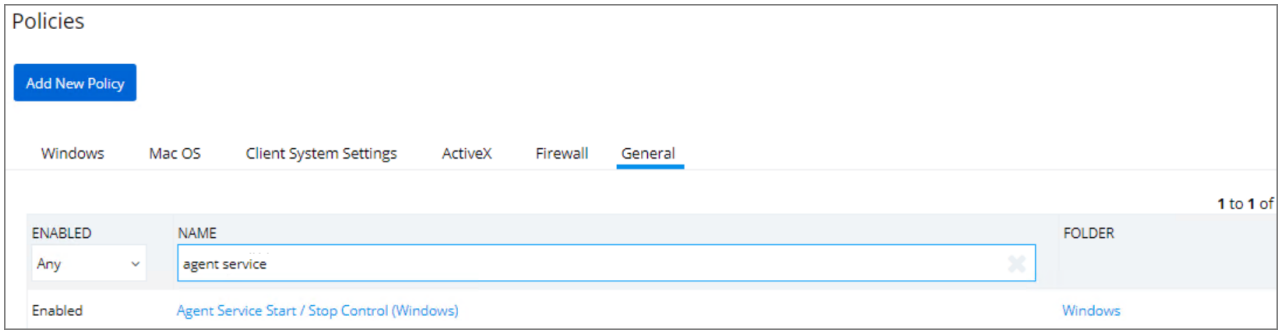


Pre-10.7.1 Agent Hardening

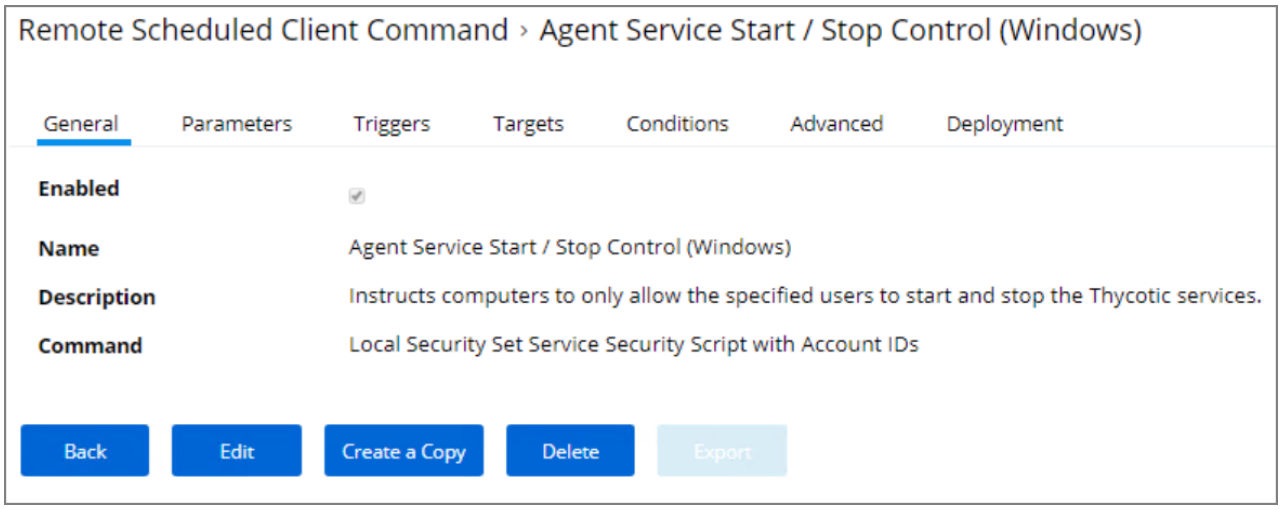
Users on Privilege Manager v10.7.1 or up should use the new policy named **Restrict Account Permissions on Agent Services (Windows)**. Refer to Agent Hardening 10.7.1 and up for details on the policy used starting with Privilege Manager v10.7.1.

Editing the Agent Service Start / Stop Control (Windows) Policy

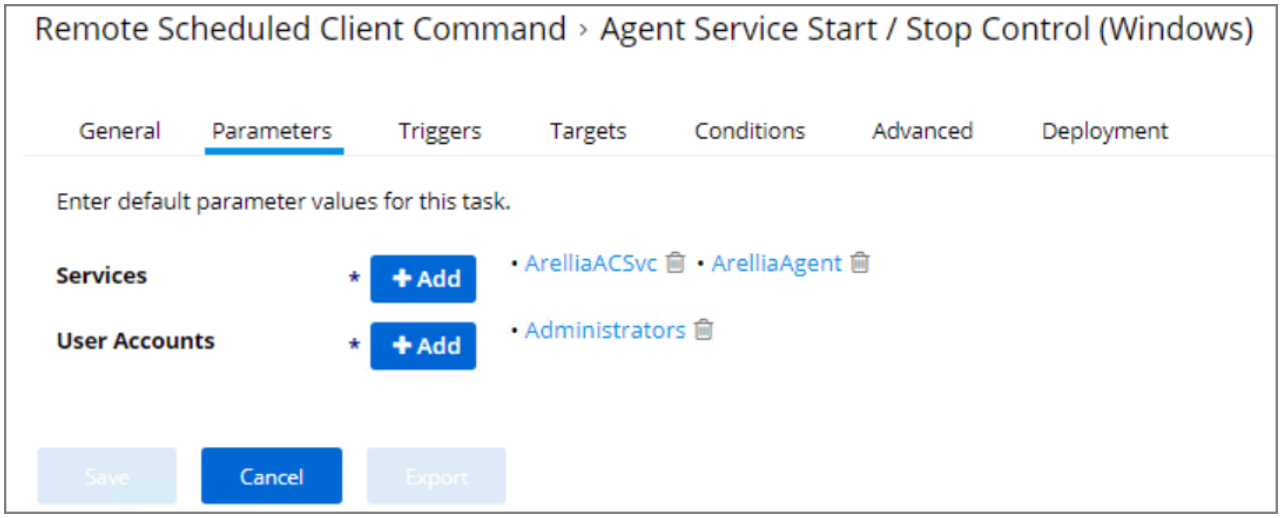
1. Navigate to **ADMIN | Policies**.
2. Click on the **General** Tab.
3. In the Name field enter **Agent Service Start / Stop Control**.



4. Click on the **Agent Service Start / Stop Control (Windows)** policy.



5. To customize the Agent Hardening policy navigate to the **Parameters tab**.
6. Click **Edit**.



7. Under **User Services** click the **+** button and use the search field to select the Services to be targeted by the task
8. Under **User Accounts** click the **+** button and use the search field to find the specific user account that has permissions to make changes to the Agent services.
9. Click **Save**.

> **Note:** If you require a rollback of the agent hardening due to upgrade issues, use the manual Restore Default Agent Permissions procedure following below.

Restore Default Agent Permissions

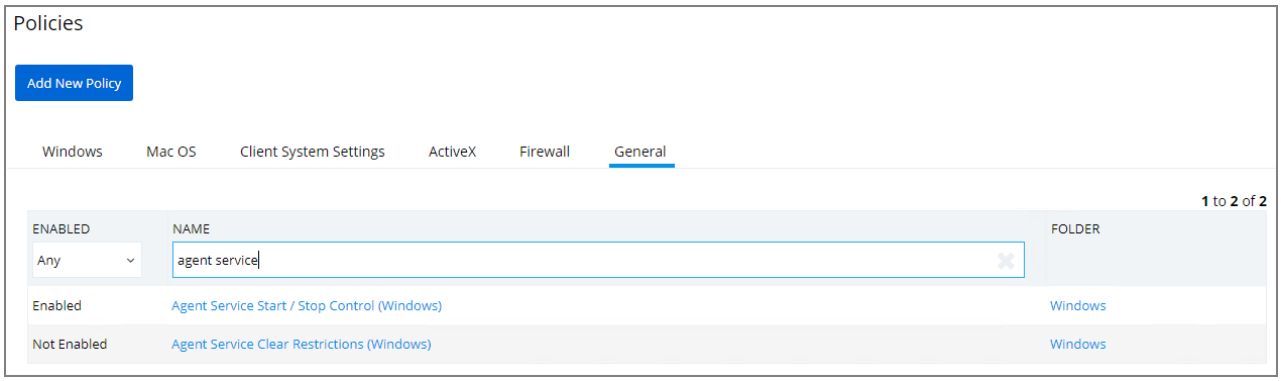
If you need to rollback agent hardening on your endpoints, follow these steps to restore the default agent permissions:

Agents

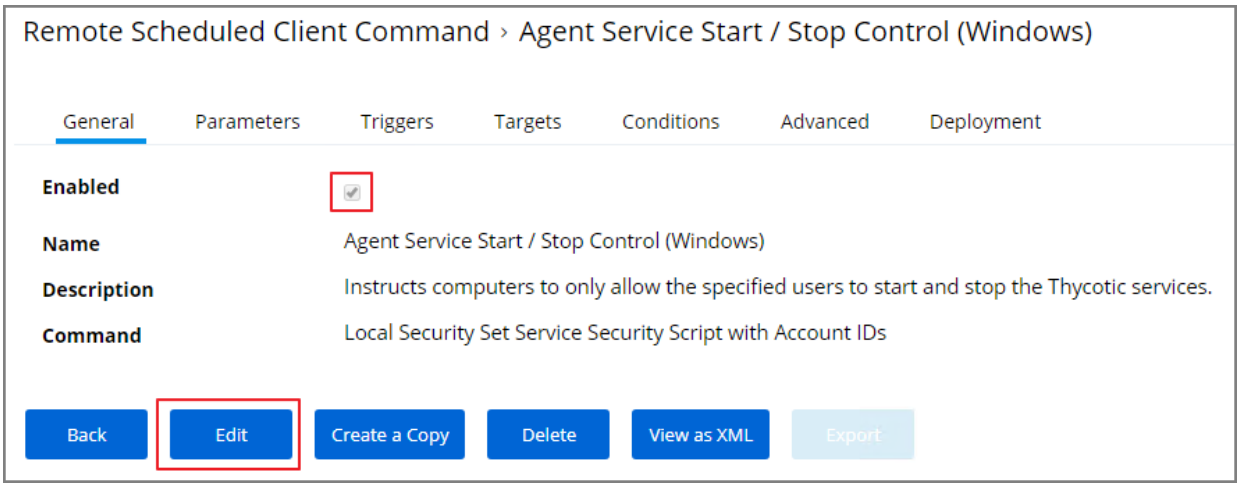
1. Navigate to **ADMIN | Config Feeds**.
2. Expand **Privilege Manager Product Configuration Feeds**.
3. Expand **Thycotic Management Server Core**.
4. Install **Reset Agent Service Permissions**.

Following the Configuration Feed installation,

1. Navigate to **ADMIN | Policies** and select the General tab.
2. Search for the agent service policies and select to edit.



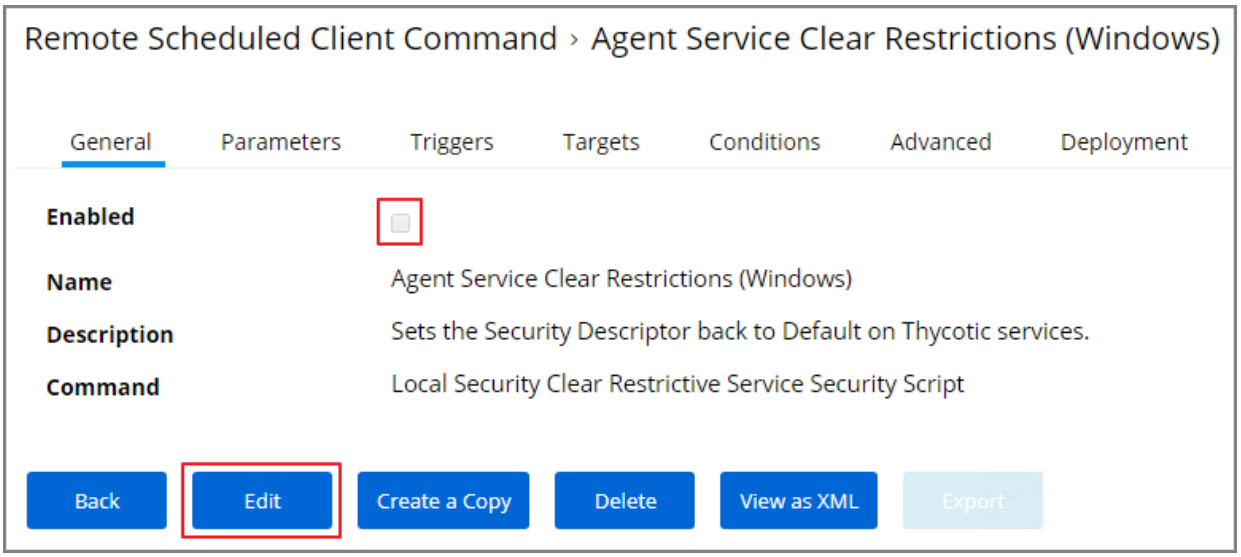
3. Disable the **Agent Service Start / Stop Control (Windows)** policy.
   a. Click **Edit**.
   b. Deselect **Enabled**.



   a. Click **Save**.
4. Enable the **Agent Service Clear Restrictions (Windows)** policy.

a. Click **Edit**.

b. Select **Enabled**.



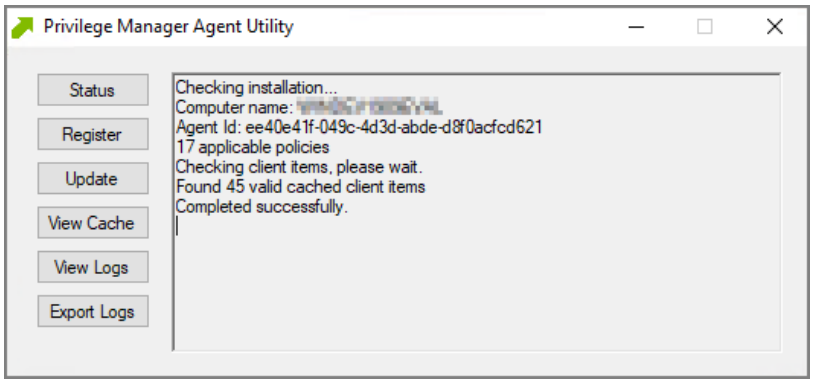
a. On the Targets tab specify the computers that need to be targeted by this policy.

b. On the Triggers tab specify when to run and/or what events will trigger the policy to run.

5. Click **Save**.

Windows Agent Utility

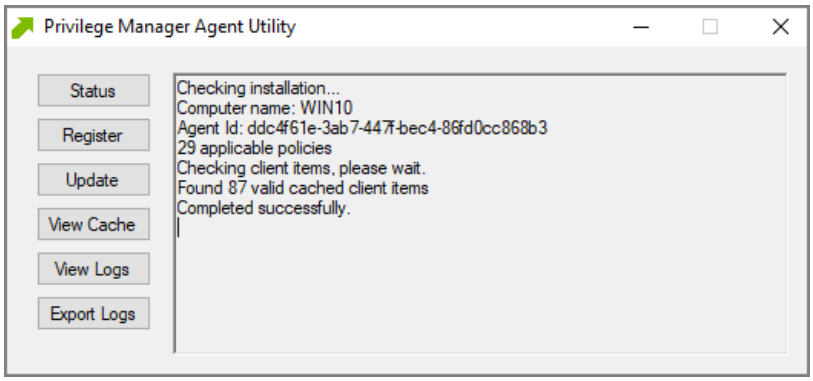
Most endpoint troubleshooting will begin with the agent. There is an Agent Utility that is installed with the agent, used to troubleshoot issues from the endpoint. To open the utility, navigate to the `C:\Program Files\Thycotic\Agents\Agent` folder on the endpoint, and run the **Agent Utility.exe** application. That will launch the utility, and it will look like the screen shot below.



Status Button

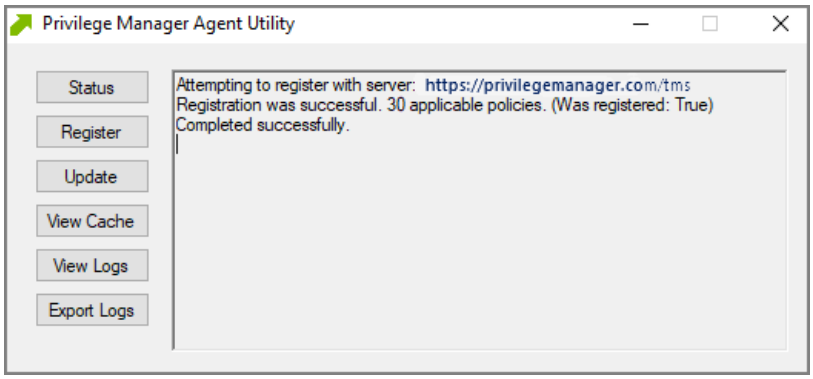
Status checks that the endpoint can communicate with the server and will show you helpful information (such as the Agent ID and how many policies the machine has) and will validate the client items cache. It is also helpful in

determining if there are any communication issues between the endpoint and the web server. This screen shot of the information shown after clicking **Status**.



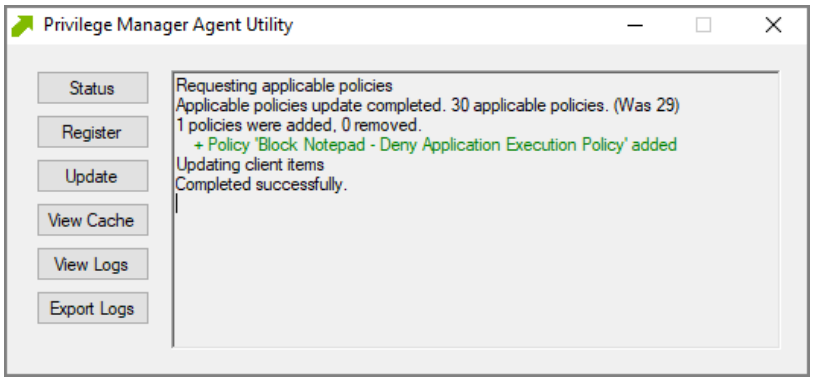
Register Button

Register attempts to register the agent machine with the web console. It shows you the URL that the machine is using to communicate with the console. It also gives errors if there are issues with that communication. If you have just installed an agent on the machine, then it also gives information about the install code if there are any errors with that.



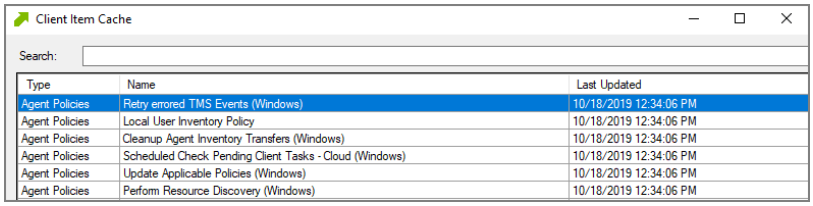
Update Button

Update communicates back to the web server and update any new applicable policies or changes to current policies, filters, actions, etc. the endpoint already has on it.

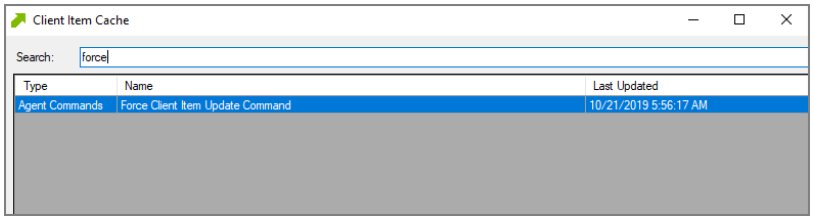


View Cache Button

View Cache opens the Agent Cache Viewer in a separate window. It displays the Policies, Filters, and Actions the endpoint has cached currently.

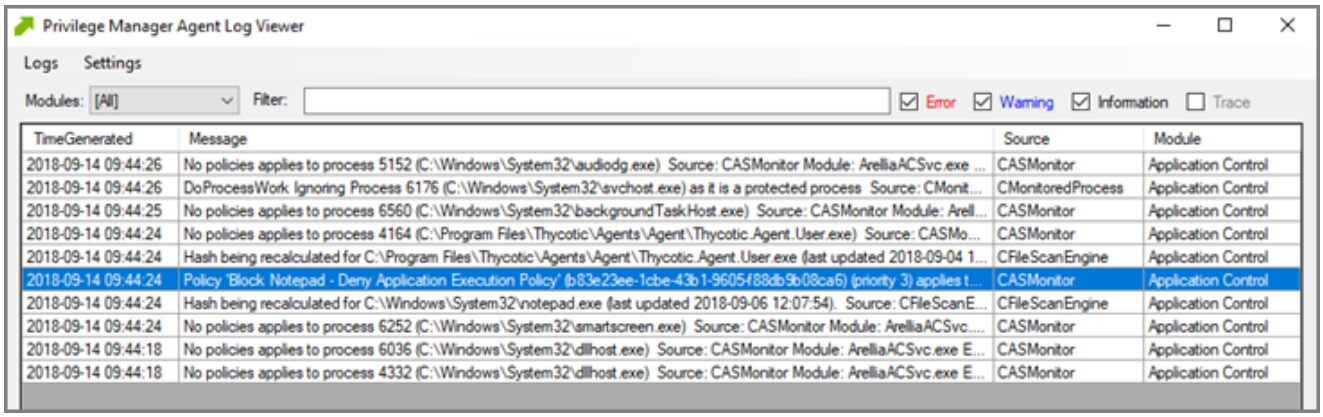


Starting with Privilege Manager version 10.7 the Client Item Cache is list also searchable. Enter a search term into the search bar and just review items that contain that term.



View Logs

View Logs opens the Agent Log Viewer in a separate window. The screen shot below shows what the log viewer looks like.

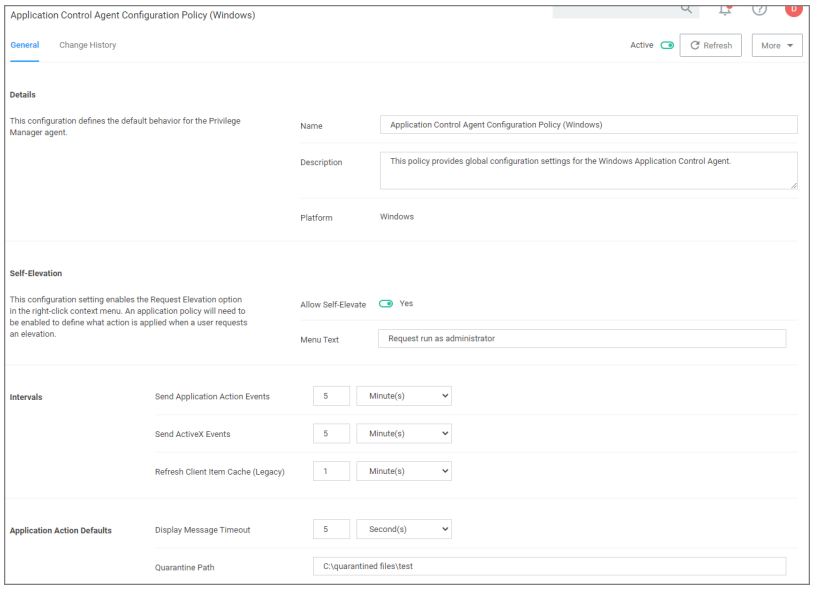


Export Logs Button

Export Logs allows you to save the agent logs so that you can send them to someone if needed. They are saved in the .evtx format so they can be opened with Event Viewer in Windows. Anytime there are issues with policies on endpoints and you need additional assistance, you will need to collect the agent logs first to help with determining what is causing the issue.

Agent Configuration

Under each Windows Computer Group administrators can specify global application control agent settings for the specific Computer Group.



- Details: This section contains the policy details such as name, description, and platform information.
- Self-Elevation: This section provides a configuration option to enable the Request Elevation option in the right-click context menu. An application policy will need to be enabled to define what action is applied when a user requests an elevation. The menu text can be customized via the Menu Text field.

- Default: Request run as administrator

- Intervals: This section provides a configuration option to customize the intervals at which the agent will send application action events, ActiveX events and refreshes the client item cache (this is a legacy items for agent version prior to 10.7.0).
  - Defaults:
    - Send Application Action Events: 5 Minutes
    - Sent ActiveX Events: 5 Minutes
    - Refresh Client Item Cache (Legacy): 1 Minute
- Application Action Defaults: This section provides the option to set the display message timeout and the quarantine path.
  - Defaults:
    - Display Message Timeout: 5 Seconds
    - Quarantine #Path: C:\quarantined files\test

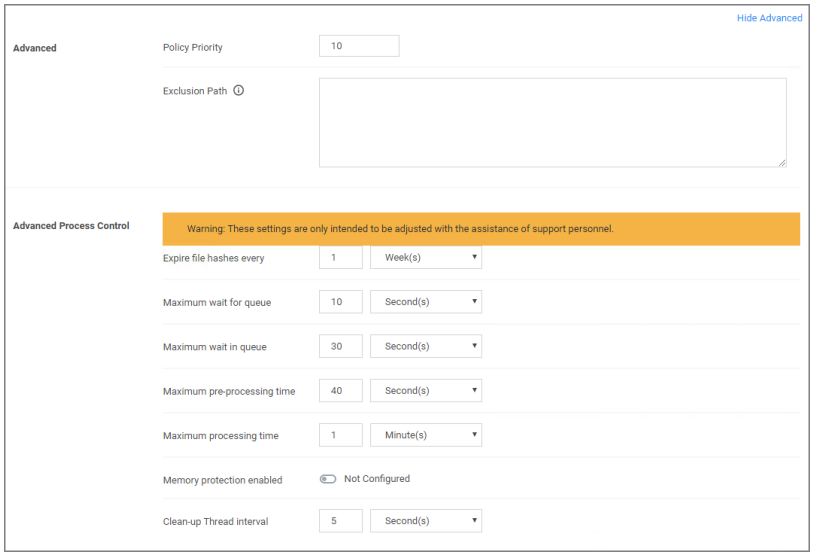
Advanced Settings

At the bottom of the page is a **Show Advanced** link.

Settings to configure:

- **Policy Priority**, this priority is specific to the Agent configuration policy.
- **Exclusion Path**, these are Global Application policy path exclusions. The setting takes the user path for each exclusion on a separate line.

Settings under **Advanced Process Control** should only be adjusted with assistance of support personnel and prior discussion of necessity for the environment.



Exclusion Path

The Agent Configuration policy can be customized to exclude specified folder paths from all application control policy processing. All applications launched from the specified paths will not be processed via the Privilege Manager agent, which allows for minimal interruption and maximum performance. Any log entries are executed asynchronously without any impact on processing.

Optimizing Compile Times

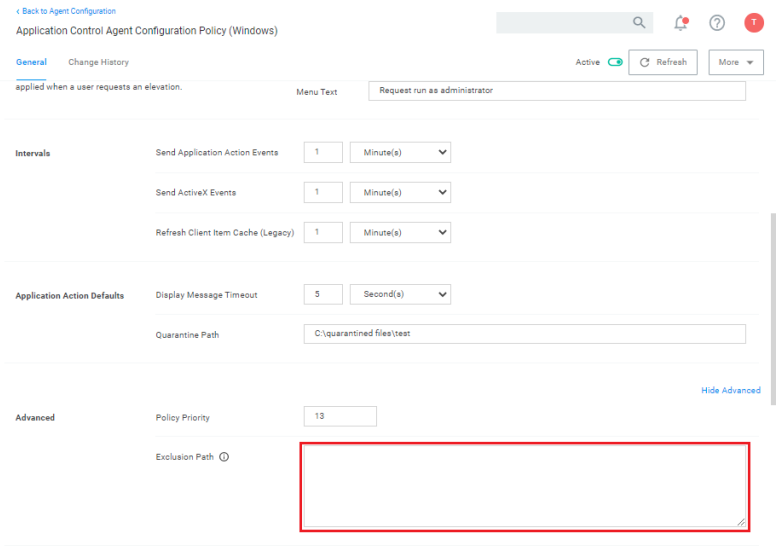
For developers with an agent installed on a computer running the {PRODUCTNAME}# application, adding an **Exclusion Path** to the application control agent is the best approach to safeguard against increased compilation times that affect system performance.

Exclusion paths are paths to software development tools (for example, program files, folders,etc.). When an application launches the agent checks the exclusions first, before filters, thereby executing faster and saving time with agent and filter assessment.

> **Note:** If performance issues persist with the use of exclusion paths, Delinea recommends an evaluation with support services to assess the environment.

To add exclusion paths to the Agent Configuration policy in the **General Settings**:

1. Navigate to your Computer Group and select **Agent Configuration**.
2. Select the **Application Control Agent Configuration Policy (Windows)** policy.
3. To access advanced settings, click **Show Advanced**.
4. In the **Exclusion Path** field, specify the path exclusions for the application control agent. Separate each path by a new line.



Verification

At the endpoint use the Agent Utility to make sure the policies are updated. Launch the application you specified in the exclusion, for out example *notepad.exe* and verify that the Agent Utility logs contain a message like this:

```
Ignoring process 11452 (C:\Windows\System32\notepad.exe) exclusion:
c:\windows\system32\notepad.exe
```

Agents Troubleshooting

Note: Generating a support file is recommended when troubleshooting with support. Refer to "Generating a Support File" below.

The following topics for agents troubleshooting are available in this section:

- Advanced Messages not working for child processes of Microsoft Edge
- Agent Registration Error Following an OS Upgrade
- Running updateclientitems.ps1 on an Agent triggers an error
- Client Item List Downloads

The following topics about Endpoint Troubleshooting are available:

- Endpoint Troubleshooting
- Catalina FileSystemWatcher Issue
- How to Recover an Unresponsive macOS Endpoint

Generating a Support File

When contacting support, Delinea recommends collecting agent related information needed to troubleshoot issues.

To do so:

1. Open the Privilege Manager Agent utility in C:\Program Files\Thycotic\Agents\Agent\.
2. Click **Support File**. This saves a zip file to the desktop. For exampe: PrivilegeManagerSupport-<*computer name*-23478765429876.zip.

3. Email the zip file to support.

Advanced Messages not Working for Child Processes of Microsoft Edge

When opting to Run an application from Microsoft Edge on Windows 10 version 1803, Advanced Messages for application justification or approval are not honored.

Detailed Information

If an application control policy targets an application such as the Google Chrome installer, the approval or justification messages will prevent the process from continuing until the message prompt is completed. However, when choosing the "Run" option when downloading an application in Microsoft Edge, the process will be created under the browser_broker.exe service and in Windows 10 version 1803 the process continues and does not wait for the Privilege Manager message to be completed.

Other versions of Windows 10 and Microsoft Edge do not appear to have this issue.

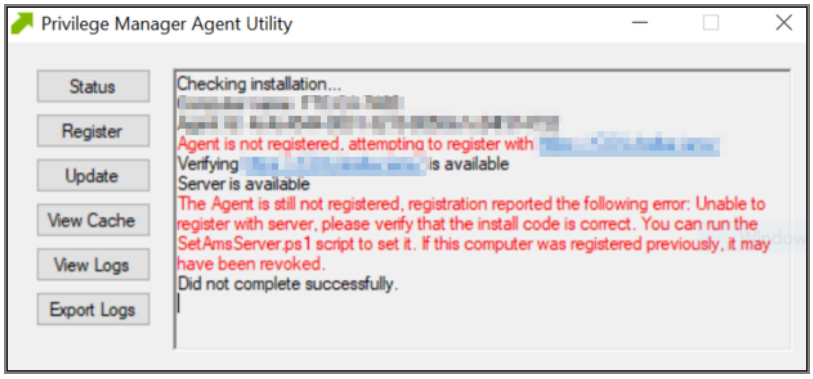
Workaround

An application control policy can be created to block browser_broker.exe and prevent users from using the "Run" option in Microsoft Edge.

Alternatively, upgrading Windows 10 will also fix the issue.

Agent Registration Issue

After upgrading, you encounter the following issue with the Agent utility after selecting "Register".



This can be caused by a Windows OS upgrade due to either a new version or build. The certificate changes and the agent will need to be re-configured for the new certificate.

Detailed Information

A. Uninstall and reinstall the agent on the machine.

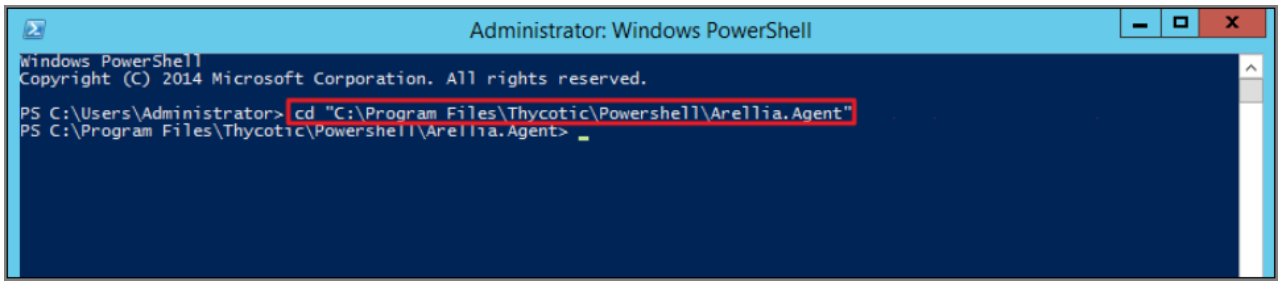
Or

B. Run the following PowerShell scripts to re-configure the agent.

Using a PowerShell Script

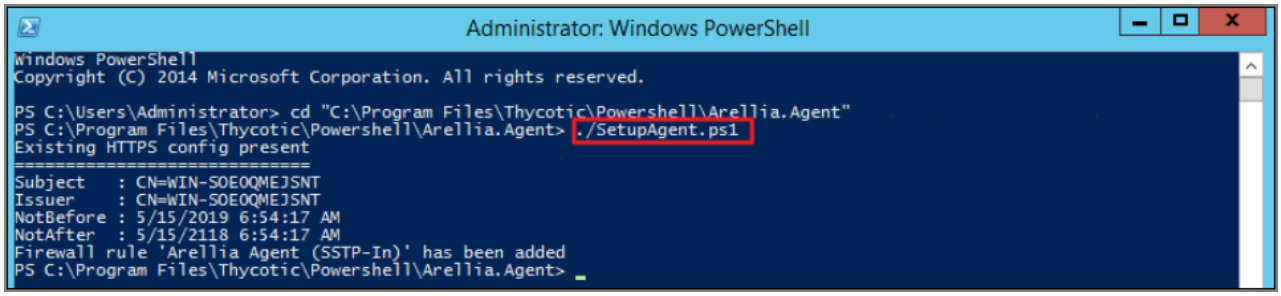
1. Right-click on **Windows Powershell** and **Run as Administrator**.
2. Enter in the following command:

```
cd “C:\Program Files\Thycotic\Powershell\Arellia.Agent”
```



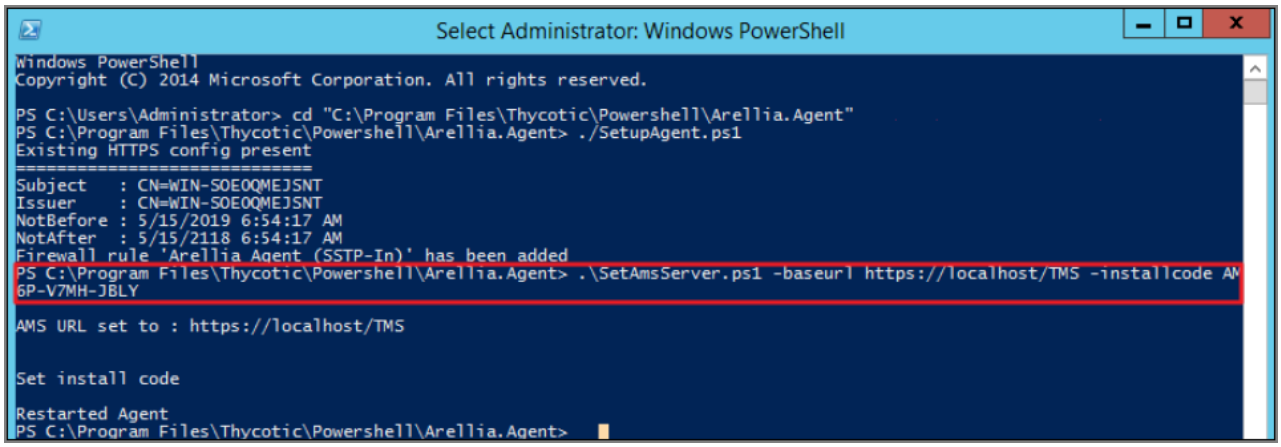
3. Enter in the following command:

```
.\SetupAgent.ps1
```

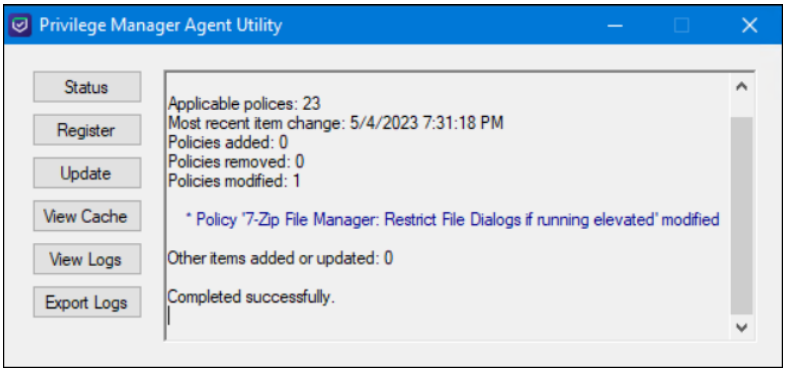


4. Enter in the following command:

```
.\SetAmsServer.ps1 -baseurl https://servername/TMS -installcode ????-????-????
```



5. Locate the Agent Utility (C:\Program Files\Thycotic\Agents\Agent\Agent Utility.exe). Open the utility and click **Update**.



Agent 404 Error: Service Startup Change

Problem

Agents will not register. The Agent log shows a 404 error: Unable to register with server: System.AggregateException: One or more errors occurred. ---> System.ServiceModel.EndpointNotFoundException: There was no endpoint listening at https:///TMS/Agent/AgentRegistration4.svc that could accept the message.

This is often caused by an incorrect address or SOAP action. See InnerException, if present, for more details. ---> System.Net.WebException: The remote server returned an error: (404) Not Found.

Navigating to https:///TMS/Agent/AgentRegistration4.svc in a browser, should show an XML response, but presents an Error 404 page instead.

Cause

SQL Server (Or SQL Server Express) and SQL Server CEIP services are set to **Automatic (Delayed)** startup instead of **Automatic**.

Solution

1. Open Services (services.msc).
2. Change both SQL Server and SQL Server CEIP to be startup type **Automatic**.
3. Ensure both services are running.
4. Open Internet Information Services (IIS) and recycle the TMS appliction pool.

The Default Web Site application may also need to be restarted on the right-hand side. If the 404 error persists, open an elevated PowerShell window and run the `iisreset` command. The error should clear and Agents should be able to register.

Agent updateclientitems.ps1 Error

While running the `updateclientitems.ps1` powershell script on a machine, you receive the following error:

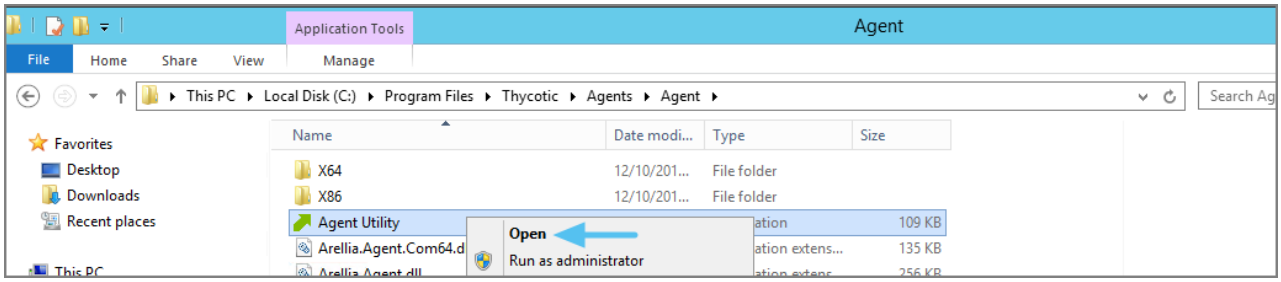
"KeySet does not exist"

```
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent> .\UpdateClientItems.ps1

============
Client Items
============

[FAILED] Downloading Windows Group Policies client item list
Keyset does not exist
```

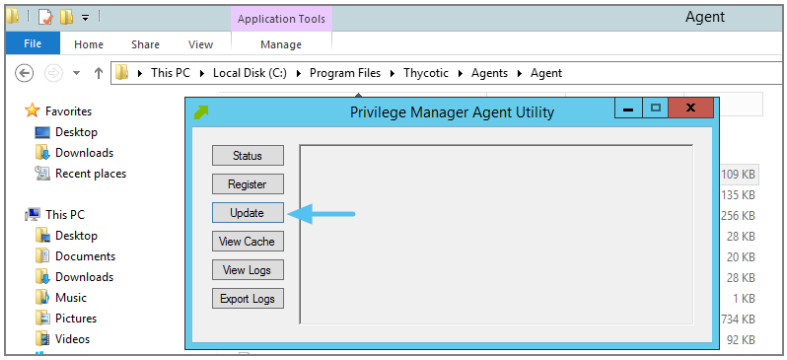
Note: The best practice to updating policies on machines would be to run the Agent Utility versus the PowerShell script. If you are still receiving the same error when using the Update button on the Agent Utility, open up a support case and include a screenshot of the error in the Agent Utility along with the agent logs.

1. Navigate to the Machine(s) where you want to update the policy and open the Agent Utility.

   `C:\Program Files\Thycotic\Agents\Agent`



2. Select **Update**.



Workstation Issues

This topic is intended to assist users in troubleshooting issues (such as policies not yielding expected results) from an workstation that has the Delinea agent installed on it.

Policy Troubleshooting

If there is an issue with policies not getting updated on the workstation, or specific files or applications not being elevated or blocked, please use the information below to help determine what is causing the issue.

Policies Not Getting Updated

If policies are not getting updated on the workstation, there could be a communication issue between the machine that has the agent installed on it and the web server. The best way to determine if there is a communication issue would be to open the Agent Utility on the workstation as described in the previous section, and then do the following:

1. Click **Status** and see if there are any errors shown.
2. Click **Register** and check for errors shown there.
3. Click **Update** and check for errors there as well.

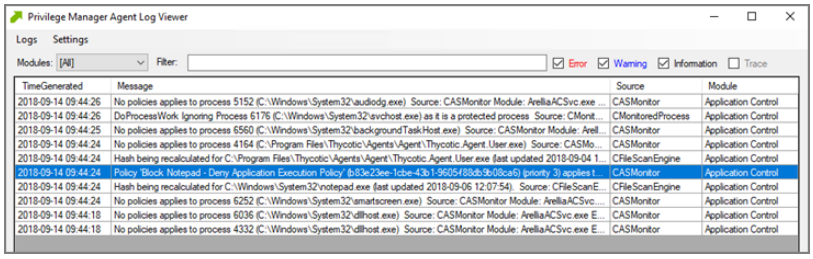
If there is an issue with the workstation communicating with the web server, there will be errors displayed in red after those selections.

Specific Files or Applications Not Being Elevated or Blocked

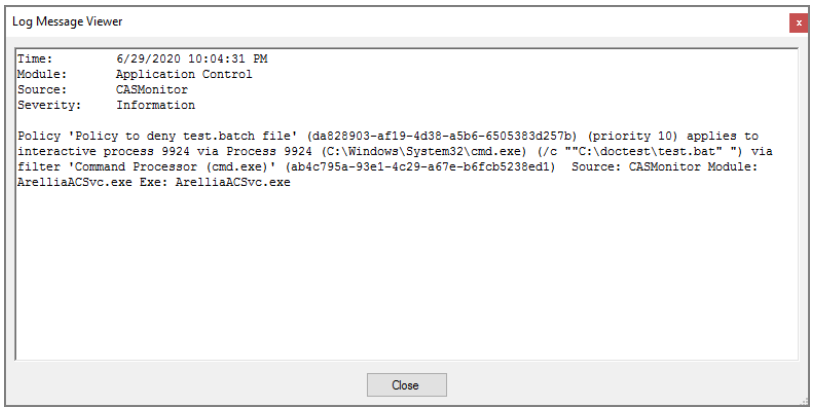
If specific files or applications are not being elevated or blocked properly, then you will need to look in the Agent Logs on the workstation. You can open the logs by first opening the Agent Utility on the workstation. Once that is open, select **View Logs** to bring up the Agent Log Viewer.

The Agent Log Viewer is very helpful for troubleshooting issues with policies not applying correctly. In the log, you can see if a policy applied to a certain process, and if so, what policy applied to that process. You can also see if there was no policy that applied to that specific process.

For example, in the screen shot below of the Agent Log Viewer, you will see a policy called **Block Notepad - Deny Application Execution Policy** that has been applied to the workstation.



The highlighted entry on this screen shot shows that the **Block Notepad - Deny Application Execution Policy** was triggered when Notepad was opened. Double-click the log entry to see further details as shown below. This shows the exact process that met the criteria of the policy and shows the priority number of that policy. The policy priority is useful information if the application continues processing through multiple policies.



With this information, you know that the policy applied to the Notepad process correctly. If there were other policies that applied to that same process, you would see them in the Log Viewer as well. There are certain situations in which clients will apply multiple policies to the same process. When troubleshooting issues with certain files or applications, the Log Viewer is a valuable tool to use.

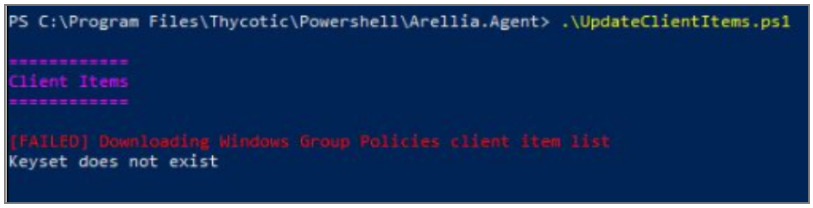
If there is no policy that applies to a certain process, the Agent Log Viewer shows you that as well. In the screen shot of the log viewer, presented above in this section, you can notice entries showing that there are some processes to which no policies apply.. Entries that begin with “No policies applies to process...” indicate that no policy was triggered when the application executed on the endpoint. If a client says that a specific file or application is not being blocked or elevated, then in the Log Viewer you can see what process is running when they launch the application and whether a policy is applying to that process.

If there are any errors in the Log Viewer, they are shown in red. Warnings are shown in blue, and Informational messages are shown in black.

Client Item List Downloads

When you run the UpdateClientItems.ps1 PowerShell script to update policies on a machine you see errors below:

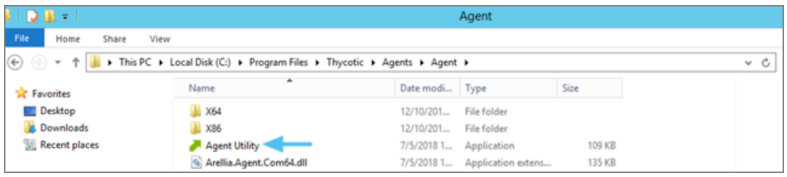
Error: *[FAILED] Downloading Windows Group Policies client item list - Keyset does not exist*

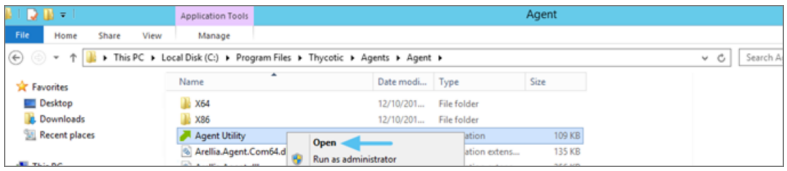


Note: This will only affect systems prior to Privilege Manager 10.7.

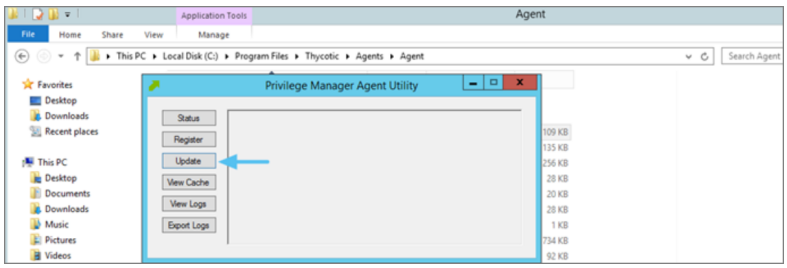
Resolve

1. Navigate to the Machine(s) where you want to update the policy.
2. Open the Agent Utility by going to `C:\Program Files\Thycotic\Agents\Agent`





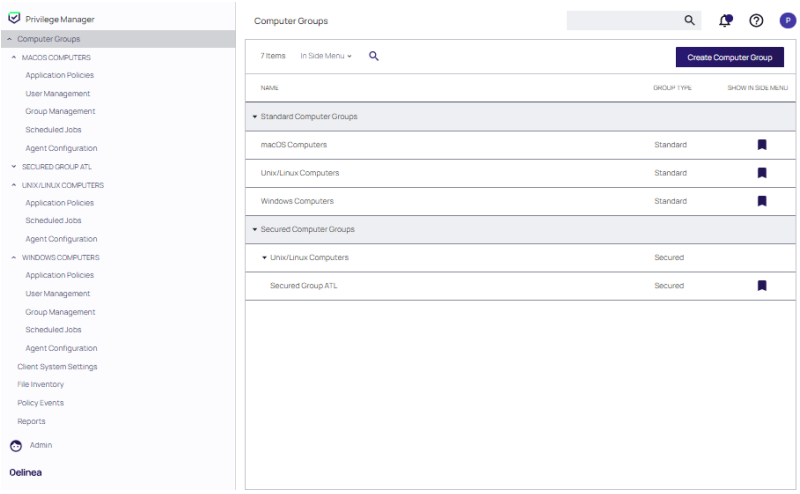
3. Click **Update**.



Computer Groups

Computer Groups organize content by platform or operating system. From each operating system, you can define Computer Groups. Click **Computer Groups** in the left navigation panel.

There a two types of computer groups as indicated by the **Standard Computer Groups** and **Secured Computer Groups** headers. A computer can be in multiple Standard groups, but only one Secured group. Secured groups can be used to apply RBAC type controls that define who can see data associated to those computers and who can create or read policies for those computers.



Standard Computer Groups

The Privilege Managerapplication provides the following three built-in Computer Groups for the **Standard Computer Groups**:

- Windows Computers
- macOS Computers
- Unix/Linux Computers

These computer groups can not be edited. Refer to Creating Computer Groups to add, customize or edit a new computer group.

Refer to Creating Standard Computer Groups for instructions.

Secured Computer Groups

Refer to Creating Secured Computer Groups for specific instructions when ccreating a Secured Computer Group.

Computer Group Management

Expand tree for any Computer Group in the left navigation. Computer Groups, called resource targets (as configured in Application Control), are specified sets of computers that meet certain criteria, that are targeted by certain policies and scheduled tasks. Each computer group addresses the following.

Default Computer Group	Resources
Windows Computers	Application Policies User Policies Group Policies Scheduled Jobs Agent configuration
macOS Computers	Application Policies User Policies Group Policies Scheduled Jobs Agent configuration
Unix/Linux Computers	Application Policies Scheduled Jobs Agent configuration

Refer to the following sections for more information:

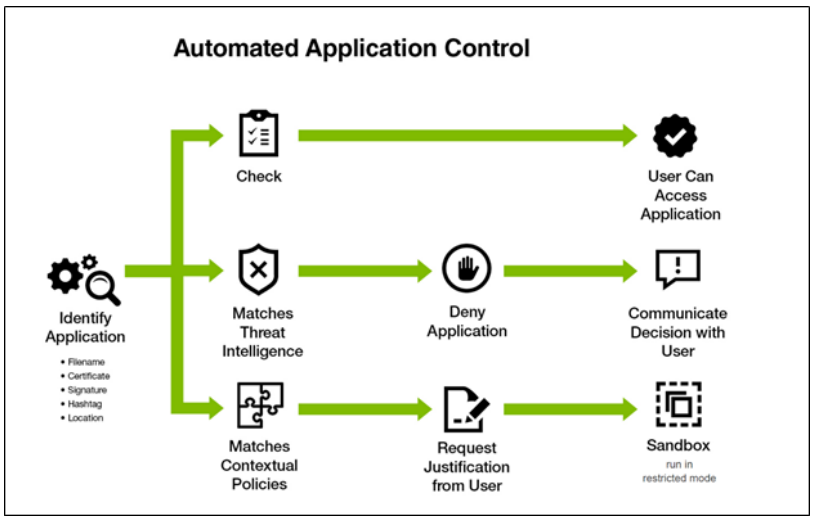
- Application Policies (Windows, macOS, Unix/Linux)
  - Policies associated with Application Control that you establish using the **Create Wizard** policy.
- User Management (Windows, macOS)
- Group Management (Windows, macOS)

- Local security control that pertains to specific groups of users.
- Scheduled Jobs (Windows, macOS, Unix/Linux)
  - Client tasks that you designate to run on certain dates and at certain times. Privilege Managersets many scheduled jobs to Active by default.
- Agent Configuration (Windows, macOS, Unix/Linux)
  - Policies that allow global configuration of agent behavior.
    - macOS
    - Unix/Linux
    - Windows

Application Policies

Application Control in Privilege Manager allows administrators to manage all application activity on endpoints. Applications requiring admin rights or root access can be automatically elevated if trusted, applications can be allowed, and malicious applications can be blocked.

In other words, the key to keeping your organization's employees working both securely and effectively without notable disruptions to their work is by tailoring a robust, role-based Application Control system. On the other hand, managing local administrator and root accounts through Local Security is the fastest way to lock down your network from malicious endpoint attacks that exploit administrator access.



Application Control

In Application Control, layered Policies create the backbone or parameters, that dictate precisely how privileges are accessed across your network. They define what a user can run, and where. A policy is made up of customizable filters that apply an action to specific Computer Groups. In other words, each policy is defined by:

- Filters - What criteria needs to be met to apply this policy?
- Targets - Where should this policy be applied?

- Actions - What should happen to the applications this policy applies to? (i.e. blocked, allowed, etc.)

During the creation of a Policy you will specify actions, targets, and filters that are created separately but then assigned to Policies.

Note: Delinea also provides default policies that can be used out-of-the-box. Refer to Default Policies.

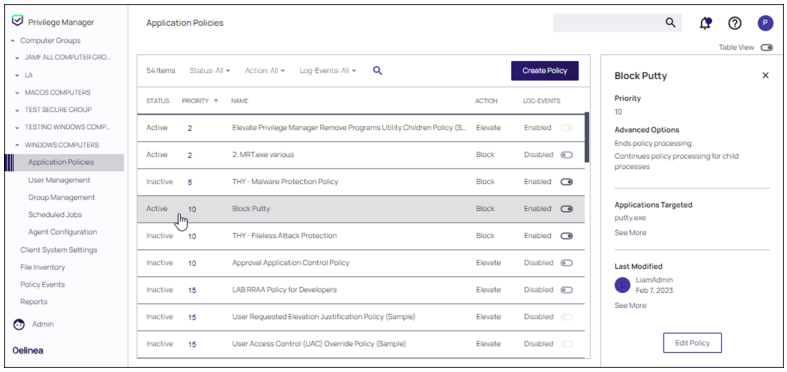
Viewing Application Policies

Identify a computer group in the left navigation panel and click **Application Policies** to view the policies defined for that computer group. Refer to Creating Application Policies to create a new policy.

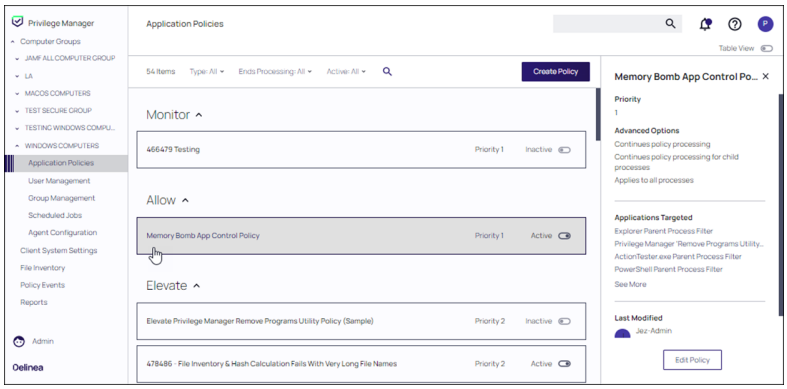
The following viewing features are available for existing policies:

- Click anywhere *outside* of the **NAME** field to open the Policy Summary panel for that policy.

  The panel that includes **Priority**, **Advanced Options** configured, **Applications Targeted** and when **Last Modified**. Click **See More** or **Edit Policy** to display the entire configuration page for that policy.



- Toggle the **Table View** control to alternate the view of policies between Table view and Card view.

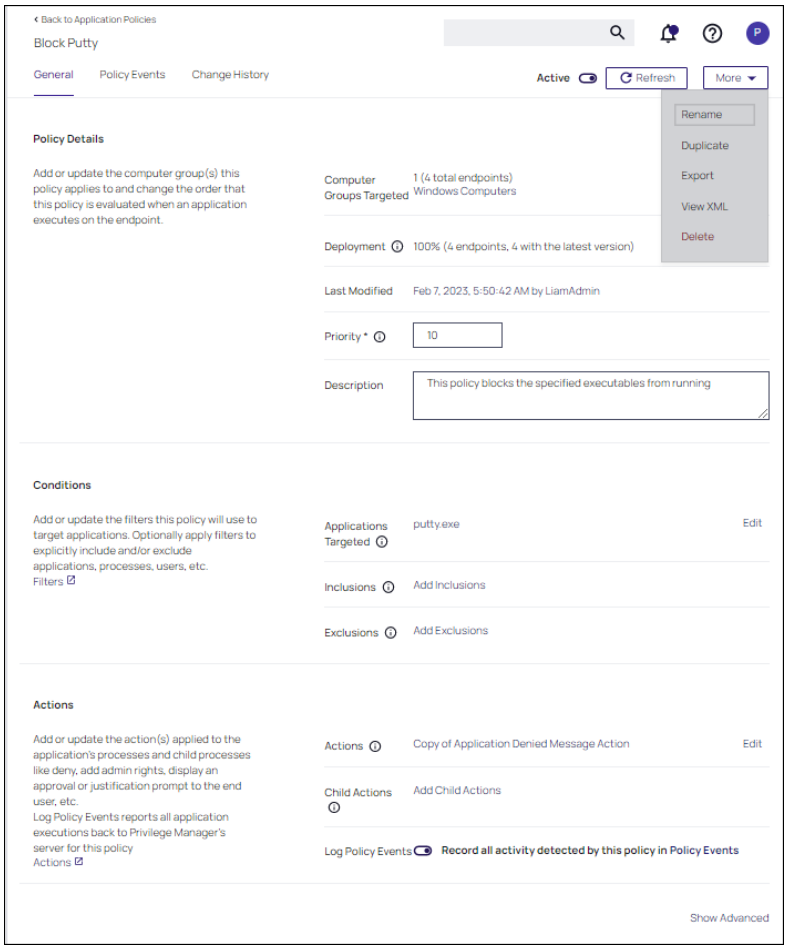


Policy Details Page

Click the name of any policy to view its Policy Details page. The following features are available:

- At the bottom of the page, click **Advanced Options** to view additional details regarding policy enforcement.
- Use the **Active** / **Inactive** toggle to change the status of the policy.

- The **More** pull-down allows you to rename, duplicate, and delete the policy. You can view XML policy settings and export policy settings as a ZIP archive file.



List of Default Policies

Here is the complete list of policies that come with Privilege Manager out-of-the-box, grouped by folder type. Once you create custom policies, they are listed along with the default policies, under the tab respective to the template used, as the template associates the folder type.

Process Hardening

Policy	Description	Type	Priority	Enabled
Remove Advanced Privileges for Interactive Users	Removes advanced privileges for users interacting with a system via Desktop	n/a	50	n

System Options

Policy	Description	Type	Priority	Enabled
Client Option - Elevate Adding Printers via Control Panel	Elevates privileges of users to allow printer drivers to be installed through the Control Panel	Elevate	60	n
Client Option - Elevate Adding Printers via PrintUI.exe	Elevates privileges of users to allow printer drivers to be installed by the PrintUI Utility	Elevate	60	n
Client Option - Elevate Changing Time and Date	Elevates privileges of users to allow them to change the system time and date	Elevate	60	n
Client Option - Elevate Device Pairing	Elevates privileges of users to allow new drivers to be installed during the device pairing wizard.	Elevate	60	n
Client Option - Elevate Disk Defragmentation (Vista/7)	Elevates privileges of users to allow them to defragment their hard disks on Windows Vista and Windows 7.	Elevate	60	n
Client Option - Elevate Disk Defragmentation (XP)	Elevates privileges of users to allow them to defragment their hard disks on Windows XP.	Elevate	60	n
Client Option - Elevate Installing Display Languages	Elevates privileges of users to allow display languages to be installed	Elevate	60	n
Client Option - Elevate Network Adapter Settings	Elevates privileges to allow user to change network adapter settings.	Elevate	60	n
Client Option - Elevate Resource and Performance Monitoring	Elevates privileges of users to allow them to run Windows Resource and Performance Monitor utilities	Elevate	60	n
Client Option - Elevate Windows Backup	Elevates privileges of users to allow them to run Windows Backup	Elevate	60	n

Privilege Management

Policy	Description	Type	Priority	Enabled
Block Script User/Group/LSA Management	This policy blocks management of local users/groups and adding/removing LSA privileges from command-line utilities, PowerShell, and their children.	Reduce	65	n
Limit Internet Browser and Mail Clients Process Rights	This policy implements the fundamental security principle of least privilege by restricting the process rights for standard Internet browsers and mail clients. Running these applications with administrative rights can present significant security problems. This policy reduces the risk of an exploit infecting a computer from within these applications.	Reduce	50	n
Limit Popular Instant Messaging Application Process Rights	This policy implements the fundamental security principle of least privilege by restricting the process rights for instant messaging applications. Running these applications with administrative rights can present significant security problems. This policy reduces the risk of an exploit infecting a computer from within these applications.	Reduce	50	n
Limit Popular Media Player Process Rights	This policy implements the fundamental security principle of least privilege by restricting the process rights for media player applications. Running these applications with administrative rights can present significant security problems. This policy reduces the risk of an exploit infecting a computer from within these applications.	Reduce	50	n
Limit Process Rights for Unclassified Applications Discovered in the Last Week	This policy implements the fundamental security principle of least privilege by restricting the process rights for an application. Unnecessarily running applications with administrative rights can present significant security problems. This policy reduces the risk of an exploit infecting a computer from within an application. This policy affects applications that have been discovered locally in the last week.	Reduce	95	n

Policy	Description	Type	Priority	Enabled
User Access Control (UAC) Override Policy	This policy allows standard users to provide a justification for elevation instead of seeing the UAC prompt.	Elevate	15	n
User Requested Elevation Justification Policy	This policy allows users to request applications to run with Administrative Rights if they provide a justification.	Elevate	15	n

Application Analysis

Policy	Description	Type	Priority	Enabled
Administrative Rights Required Detection Policy (Application Compatibility)	This policy detects applications that are deemed to require Administrative rights by Windows.	Elevate	45	n
Administrative Rights Required Detection Policy (Security Manifest)	This policy detects applications that contain a security manifest that specifies administrative rights are required.	Elevate	45	n
Event Discovery Audit Elevated Privileges Policy	This policy will detect all applications that are run with Administrator Rights on endpoints with the agent. This policy can be configured on the Event Discovery Configuration page.		45	n
Setup Detection Policy	This policy reports on applications that are detected as an installer.		45	n

Windows Policies

Policy	Description	Type	Priority	Enabled
Event Discovery Testing Computers Audit Policy (Windows)	This policy is enabled through the Event Discovery configuration by enabling the option to log all activity from the test group.	97	n	
Elevate Privilege ManagerRemove Programs Utility Policy	This policy needs to be enabled if users are supposed to be able to remove programs and apps via the Remove Programs Utility.	2	n	

macOS Policies

Policy	Description	Type	Priority	Enabled
Event Discovery Testing Computers Audit Policy (macOS)	This policy is enabled through the Event Discovery configuration by enabling the option to log all activity from the test group.		97	n

Automatic Elevation via Windows Client System Settings

Common Windows client settings can be deployed to endpoint agents the same way as any policy. These settings target **All** Windows Computers with Application Control Agent Installed (Target)" as the default resource target. Once a setting is selected from the list, the resource target can be modified to include specific computer or other existing resource targets can be assigned on screen.

Policy	Description
Add Devices	Allow users to add drivers, installing drivers as necessary.
Add Printers	Allow users to add printers, installing drivers as necessary.
Backup the System	Allow users to perform system backup operations.
Change the Date and Time	Allow users to change the date, time and timezone.
Change Network Adapter Settings	Allow users to change the network adapter settings.
Defragment the Disk	Allow users to perform disk defragmentation operations.
Install Language Packs	Allow users to install operating system display languages.
Monitor Performance	Allow users to run the Windows Performance Monitor utility.

ActiveX

ActiveX Setting define which sites can run ActiveX controls for standard users.

To create an ActiveX setting, a new policy must be created based on the ActiveX policy type template.

Note: You will need to import local group policy definitions before editing your Active-X Group Policy Settings.

Firewall

An Application Firewall Policy policy type allows for firewall rules to be applied as an Action in an Application Control Policy.

To create Firewall rules, a new policy must be created based on the Windows Application Policy type template.

When defining the Firewall Policy an Application Classification must be set. An Action of type Application Classification can then apply that classification to an Application Control Policy, which then enforces all of the defined Firewall Policies that are defined with that classification.

General

The policies available on the General tab are covering the basic Privilege Manager functionality and are enabled by default. Most of these policies are fulfilling utility functions otherwise also considered tasks.

Policy	Description
Basic Inventory (Initial, macOS)	This scheduled task triggers the Agent to send macOS basic inventory. This policy takes an inventory as soon at the agent and the initial policies are deployed and should be removed from the machines afterwards.
Basic Inventory (Initial, Windows)	Instructs computers to report the Win32_ComputerSystem, Win32_ ComputerSystemProduct and Win32_OperatingSystem WMI classes to the server. This policy takes an inventory as soon at the agent and the initial policies are deployed and should be removed from the machines afterwards.
Basic Inventory (macOS)	This scheduled task triggers the Agent to send macOS basic inventory.
Basic Inventory (Windows)	Instructs computers to report changes to their Win32_ComputerSystem, Win32_ ComputerSystemProduct and Win32_OperatingSystem WMI classes to the server on a scheduled basis, like once a week for example.
Cleanup Agent Inventory Transfers (Windows)	Completes and cleans BITS transfers and temporary files used by the TMS Agent Inventory Helper.
Cleanup sent Privilege ManagerEvents (macOS)	Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.
Cleanup sent Privilege ManagerEvents (Windows)	Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.
Default File Inventory Policy (macOS)	The purpose of this policy is to inventory software programs running on the managed computer.

Policy	Description
Default File Inventory Policy (Windows)	The purpose of this policy is to inventory software programs running on the managed computer.
Ensure UAC Override Setting (Windows)	Ensures that the UAC Override Registry Key is set.
Local User Inventory Policy	The purpose of this policy is to inventory Local User account, groups and group membership on the client. This policy can also be used to inventory for specific account privileges.
Local User Inventory Policy (macOS)	The purpose of this policy is to inventory Local User account, groups and group membership on the client. This policy can also be used to inventory for specific account privileges.
Perform Resource Discovery (macOS)	Schedule on which agents will check with server to determine if any local resources require discovery.
Perform Resource Discovery (Windows)	Schedule on which agents will check with server to determine if any local resources require discovery.
Retry errored TMS Events (macOS)	Scan Agent queue for any events that require retransmission.
Retry errored TMS Events (Windows)	Scan Agent queue for any events that require retransmission.
Scheduled Check Pending Client Tasks - Internet Clients (Windows)	Initiate a check for pending client tasks. Used by agents that are unable to receive an incoming connection from the server.
Scheduled Registration - Internet Clients (Windows)	Initiate agent registration with server less frequently than internal clients.
Scheduled Registration (macOS)	When this policy is triggered the Agent will attempt (or re-attempt) to register with the server.

Policy	Description
Scheduled Registration (Windows)	Initiate agent registration with server.
Update Agent Commands (macOS)	When this policy is triggered the Agent will update agent command items.
Update Agent Commands (Windows)	Instructs Agent to update any agent commands if required.
Update Applicable Policies (macOS)	When this policy is triggered the Agent will check the server for updated policies.
Update Applicable Policies (Windows)	When this policy is triggered the Agent will check the server for updated policies.
Update Applicable Policies - Internet Clients (Windows)	Instructs Agent to check with server for policy changes less frequently than internal clients.
Update Provisioned Resource Client Items (macOS)	
Update Provisioned Resource Client Items (Windows)	
User Logon Inventory Policy	Updates user logon data on the given schedule.
Windows Service Inventory Policy	The purpose of this policy is to inventory Windows Services on the client.

Not Enabled

Policy	Description
COM Inventory Policy	The purpose of this policy is to inventory COM+ and DCOM packages installed on the client.

Policy	Description
Disable Local Guest Accounts	Provisioning policy to disable local Guest accounts on Windows computers.
Randomize Administrator Password	
Shared Folder Inventory Policy	The purpose of this policy is to inventory shared folders on the client.

Before You Begin with Policies

Creating policies follows a configuration process. Review the following information prior to configuring an application policy.

Using the Configuration Process

While there are many different types of policies, the setup process must follow these basic steps:

1. Collect File Data - This enables Privilege Manager to recognize specific files and file types in your environment. The file data that you want to target with policies are called Events. All imported files can be viewed under **File Inventory**.
2. Create Filters - This step sorts important file data (Events) according to different criteria.
3. Create Policies - This step defines what

   a. Actions to perform on applications and the

   b. Targets (Locations) for those actions.
4. Assign Filters to Policies - This step directs a Policy's actions to the appropriate Events happening on your network.
5. Order your Policies based on priority level - Once your policies are created, the order they execute across your network matters. See the Policy Priority section in this guide for more details.

Collecting File Data

Before Privilege Manager can do anything else for Application Control, it must be able to recognize files or file types in your environment like applications or executables that run. File data can be collected in several ways:

- Event Discovery - Discover active applications on your network by setting up Learning Mode Policies
- File Upload - Directly upload a specific file that you want to target
- Remote File Inventory Task (Windows/macOS) - Scans endpoints directly and imports all file data (both active and inactive files) that exist on the targeted machine(s)

Points to Consider

If you configure Privilege Manager policies incorrectly they could prevent services or programs from starting or running with the proper rights.

Policies are evaluated in order based on the Policy Priority value on the Policy. If a blocking policy that denies applications is too broad and is set with too high a priority, it can unintentionally prevent other applications from running or letting the user request approval to run.

You can avoid conflicts resulting from incorrectly configured Privilege Manager policies by using the following best practices:

- Always test policies on machines which mirror the production environment before rolling out to production.
- Assign policies that allow processes a lower policy priority number than policies that deny processes.
- Make sure your other policy enforcement settings check boxes are selected or cleared, depending on the aims of your policy.
- Policies that deny processes always exclude the following application filters:
  - LocalSystem and Service
  - Signed Security Catalog
- You should (almost) never use wildcards in deny policies. Wildcards should be considered only after performing extensive testing.
- Do not add User Context filters as the only application target to a policy. Starting with Privilege Manager version 11, the UI does alert to this as being an invalid policy. Refer to Warning Banner indicating Filter Error Conditions in Policies.

Creating Policies

Two types of policies can be created: monitoring policies and controlling policies. Monitoring policies only report on the fact that an application was run, while controlling policies will actually intercede in some manner, such as elevating, restricting, blocking, requiring justification/approval, etc.

Within policies, there are subtypes. Subtypes are associated with the types of actions that they are configured to use. A wide variety of subtypes can be created, such as managed [local] users, managed [local] groups, service hardening, etc. For example, if the policy has an **Add Administrative Rights** action, it's an elevate policy. If it has a **Deny Execute** action, it's a block/deny policy, etc.

Policies can be created using any of the following methods:

- Policy Wizard
- Workstation Policies
- Policy Templates

Note: Once a policy is created, it must be activated; and if desired, customized further. Refer to Activating_and_Customizing_a_Policy.

Using Policy Templates

Privilege Manager ships with most commonly used policy templates. These are utilized by the policy wizard when creating a new policy.

Delinea also provides templates that do not ship with the product, but that can be downloaded via Configuration Feeds from within the Privilege Manager Console. Once downloaded and installed, customers can access those policy templates via Admin | Folders. Here a new policy can be created based on a template from a drop-down list.

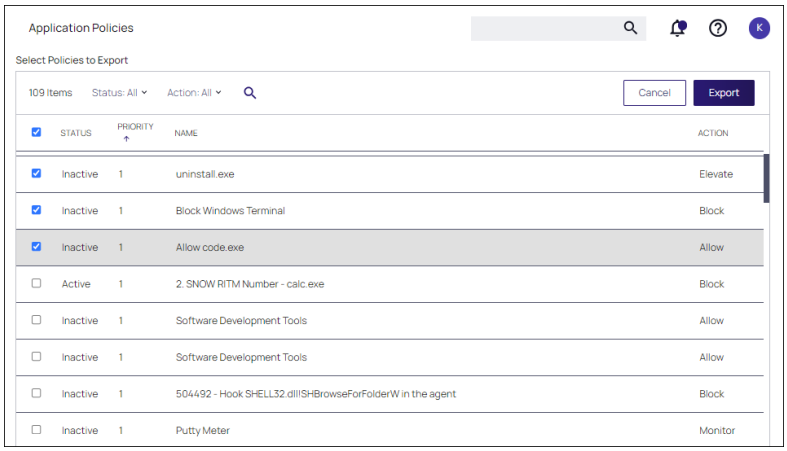
This policy will have associated targets, filters, and actions set, which can be further customized to cover an organization's specific needs. Also refer to Configuration Feeds.

Exporting Policies

Application policies can be exported from the Application Policies page. Prior to exporting a policy, consider:

- If you are exporting policies associated with a custom Computer Group that have been moved to another Privilege Manager instance, you first need to import the Computer Group to allow you to then import the associated policies.
- If you are exporting policies associated with a custom made Secured Group that have been moved to another Privilege Manager instance, you first need to import the Secured Group, its Security Descriptor and Resource Target to allow you to then import the associated policies.

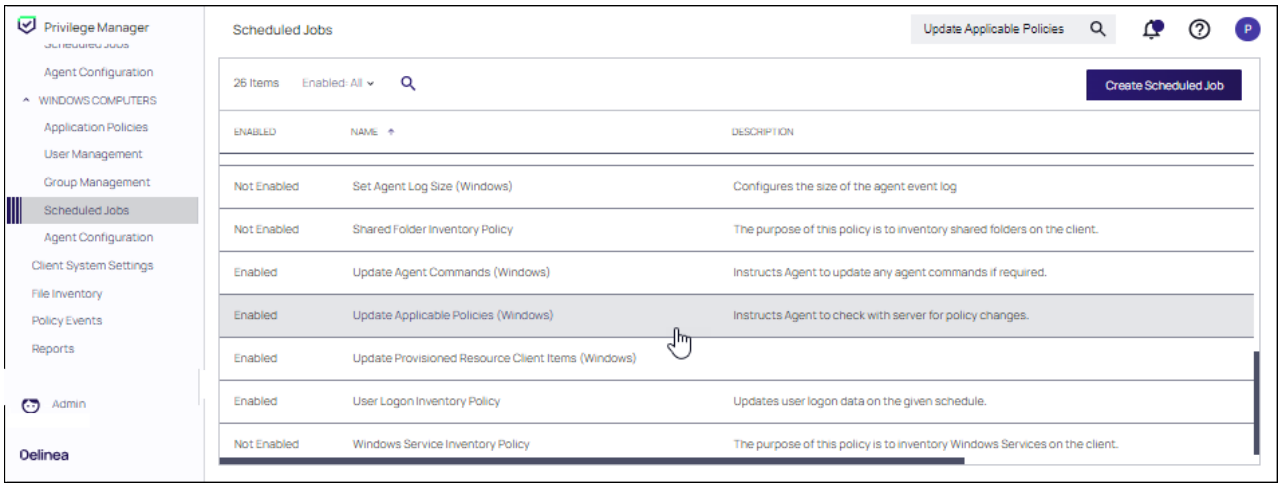
1. Navigate the Applications Policies page in your Computer Group and select **Export**.
2. Enable the check boxes next to each policy to be exported. A select all check box is also available.
3. Click Export.



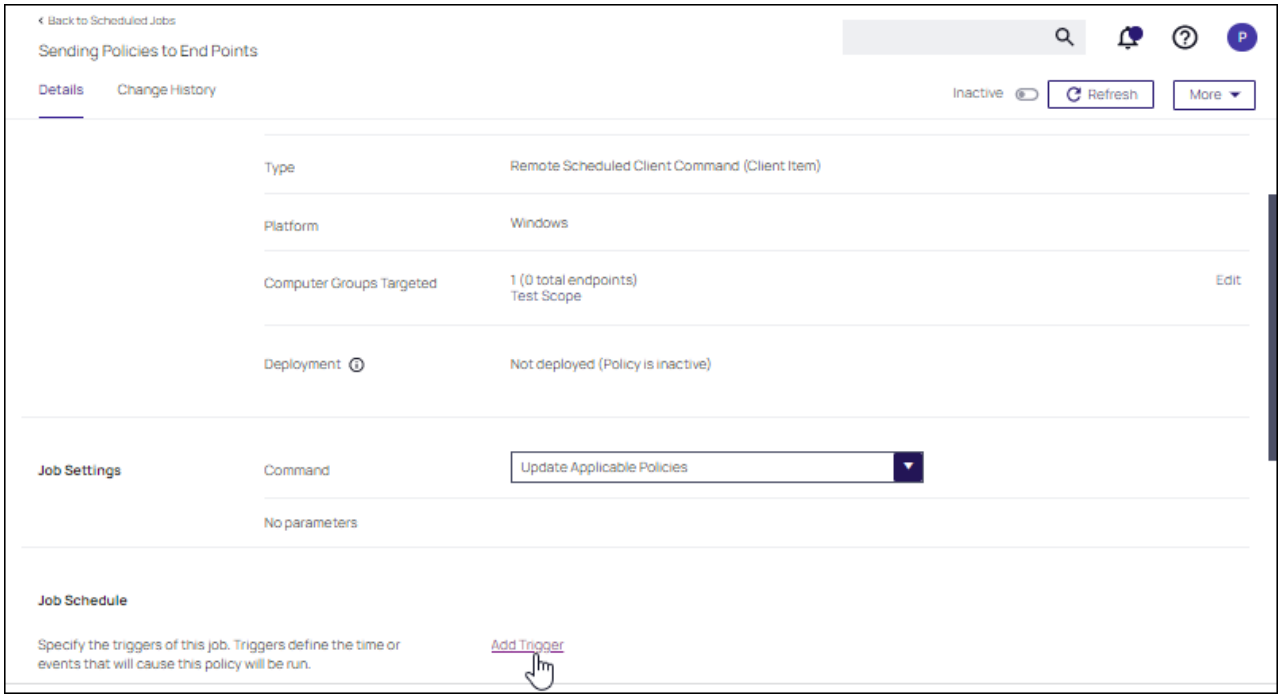
Sending Policies to Workstations

After setting up your first policies, keep in mind that even after you enable them, new policies are not immediately sent to target endpoints (workstations). Instead, policies are updated on workstations via the schedule defined by the Update Applicable Policies task. By default this tasks runs once daily.

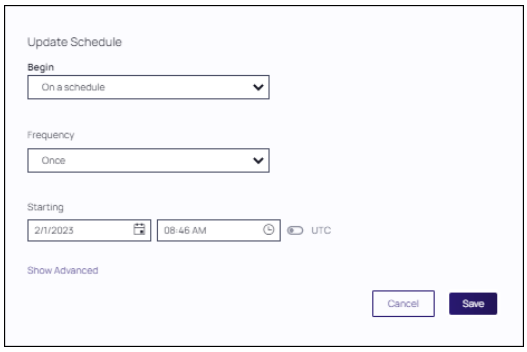
1. In your Computer Group, select **Scheduled Jobs**.
2. Search for the *Update Applicable Policies* task:



3. Select the **Update Applicable Policies (Windows)** for example.
4. To edit the time scheduled that sets off this task, under Job schedule click **Add Trigger**.



a. Select to run this schedule **Once** on demand and make sure the time indicated is in the future. Click **Show Advanced** for more options for the modification.



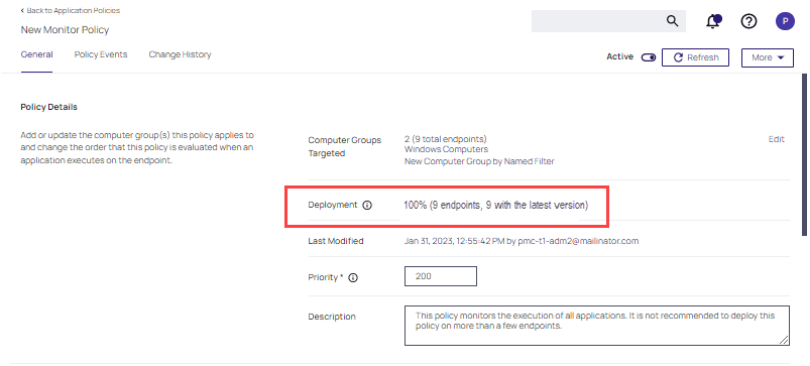
In production environments having a delayed deployment schedule prevents performance issues when adjusting policies and rolling them out across a large number of agents on your network. However, when setting up new policies you may want to immediately activate them on testing workstations and verify your configurations are working correctly.

5. Click **Save**. The data under **Job Schedule** indicates to run once.

6. Click **Save Changes** for the modification to take effect.

View Deployment Status

Within a Policy's Detail View, verify the deployment status. This will tell you how many computers the policy is already deployed on:



Note: If the deployment status number is 0 or incorrect, it is possible that the *Resource and Collection Targeting Update* task needs to run.

Update Policies on an Endpoint using Powershell (prior version 10.7)

On Privilege Manager version prior to 10.7, the fastest way to deploy or update your policies on a specific testing workstation is by running a simple Powershell script directly on your test machine where a Delinea Agent is installed.

1. On your workstation, right-click on the Windows Powershell application and select **Run as Administrator**.
2. Navigate to the Agent directory by entering the following command and then enter:

```
cd "C:\Program Files\Thycotic\Powershell\Arellia.Agent"
```

3. Next type:

```
UpdateClientItems.ps1
```

4. Press Enter.

Note: If your policies are not immediately updated, wait a few minutes and try running the script again.

After you've updated your test workstations, you can try running applications that are targeted by your policies to make sure the policies are configured correctly. You will also see the policy's Deployment status information updated, if refreshed.

Agent Event Log Viewer

Another helpful place to look when setting up new policies is your Agent's Event Log Viewer. On your workstation:

1. Navigate to your Delinea Agent files. This is usually located in `C:\Program Files\Thycotic\Powershell\Arellia.Agent`.
2. Right-click on **AgentLogViewer** and select **Log Viewer**. The Agent Event Log Viewer displays and shows updates in real time, as the agent communicates with the Privilege Manager server. For remote access, Agent logs are also viewable through the Windows Event Viewer.
3. Scroll to the top of the page to see the most recent activity from your Delinea Agent.
4. Deselect **Information** in the upper right-hand corner to narrow search results for any Errors and Warning messages that may be occurring. You can also double-click any line item for more detailed information about each event.

Now that you know how to update your workstations and check to make sure your policies are working, it's time to start building new policies!

Just In Time Elevated Access

Just In Time (JIT) elevated access is used to grant temporary administrator access to workstations without having to create unique policies for applications with this need. Normally, policies only apply to certain applications, but in JIT mode, any application that requires elevation can be run as Administrator by the user.

Important: JIT elevation is supported on agent versions 11.4.2 and later. Assigning this policy to older agents will cause ALL policy processing to fail.

Three policies are involved in setting up JIT functionality. They are:

- JIT Mode (Startup and Approval) (Sample) - applies to the JIT mode helper application.
- JIT Mode (Sample) - handles elevating access while JIT elevated access mode is running.
- JIT Mode (Child Processes)(Sample) - tracks applications to ensure that everything run during JIT mode is shut down at the end of the approved time limit.

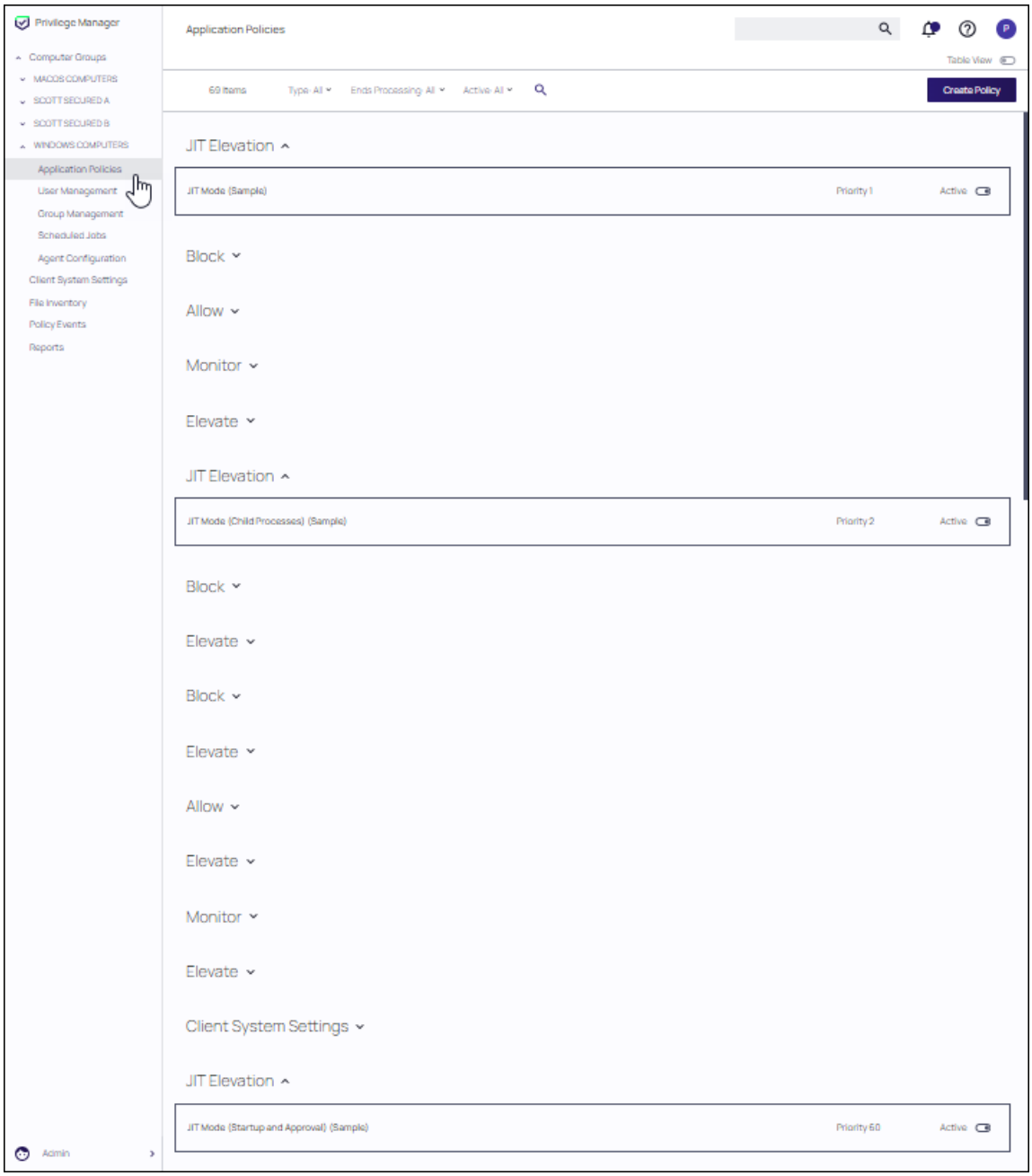
Configuring JIT Mode

Enable the JIT Mode policies

Navigate to the Application Policies in the default Windows Computer Group and locate each of the three JIT Mode policies. Click the **Active** toggle to activate each policy.

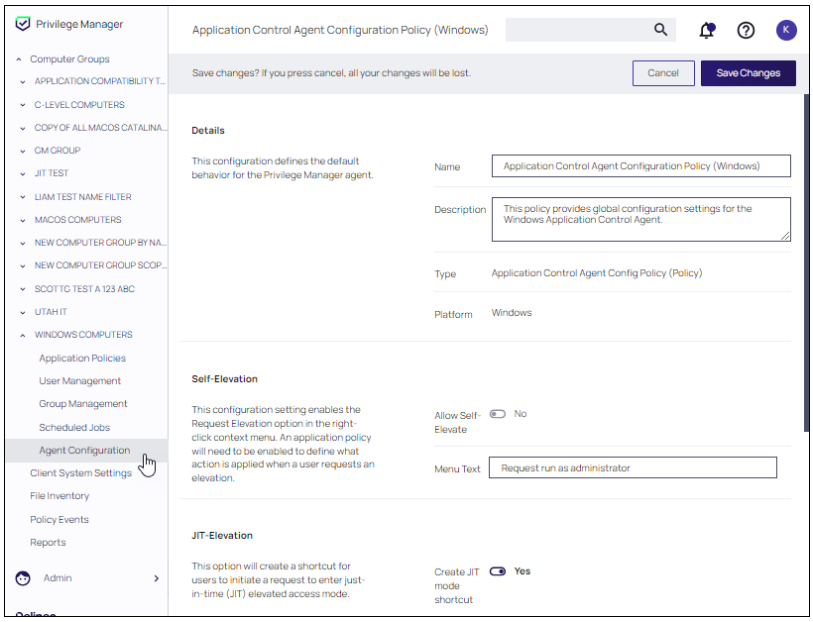
To assign the default JIT policies to another Computer Group, duplicate, then edit the default JIT policies.

Computer Groups



Enable the JIT mode shortcut

Navigate to **Agent Configuration** and set the **Create JIT mode shortcut** toggle to **Yes**.



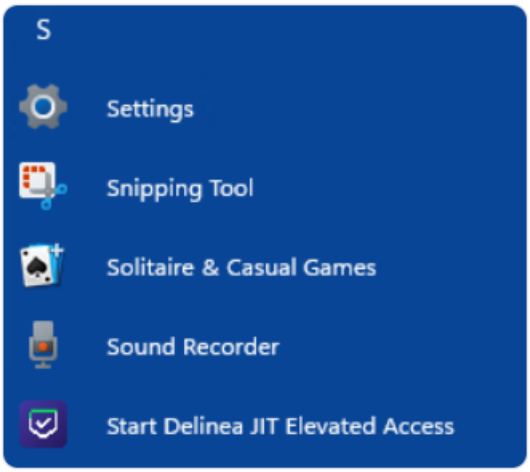
Using JIT Mode

Requesting JIT mode

You use a shortcut to enter into JIT mode elevated access for your agent. Find the **Start Delinea JIT Elevated Access** shortcut and select it to initiate an approval request for JIT mode. For Windows 10 workstations, the shortcut is listed in the top level of the programs list. For Windows 11 workstations, the shortcut is listed in the **Delinea** folder.

Your request for elevated access is sent for approval.

Windows 10

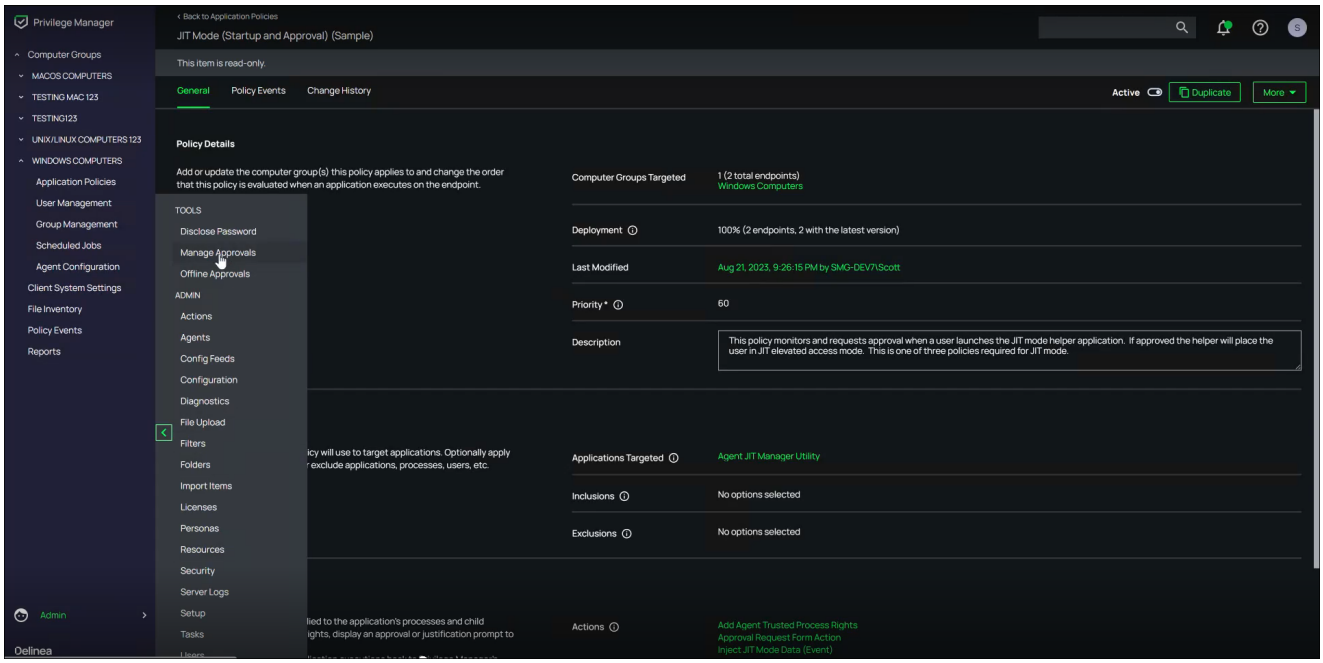


Windows 11

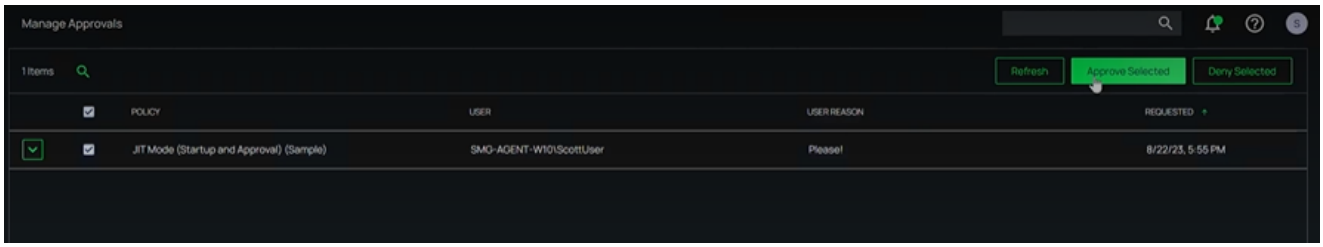
(Admin) Approving a JIT Request

Administrators receive requests for JIT elevation and need to approve those requests.

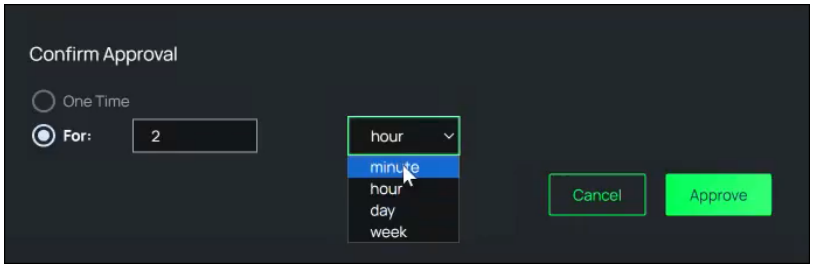
If you are an Administrator, navigate to **Admin** | **Manage Approvals**.



Enable the JIT Mode (Startup and Approval)(Sample) policy and click **Approve Selected**.



Select the **For** option and set the time for the elevated access and click **Approve**. (The **One Time** access is only in instances where you need to use a default elevation time of 30 minutes.)

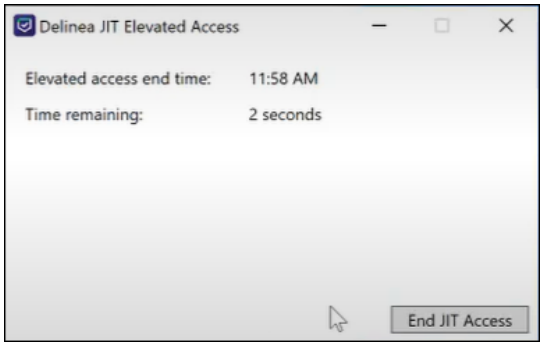


Working as Administrator in JIT Mode

Once approved, a Windows notification appears, indicating that JIT elevated access has started. You can now run any application of your choice as an Administrator.

Periodic Windows notifications appear during elevation as a reminder of time remaining. Additionally, an icon appears in the system tray. Click the icon to see the time remaining in JIT mode. If desired, click **Exit JIT Access** to end elevation mode early.

> **Important:** Carefully monitor the time remaining in JIT mode. At the end of the approved time, any application elevated as part of JIT mode will be terminated, and may result in the loss of any unsaved work.

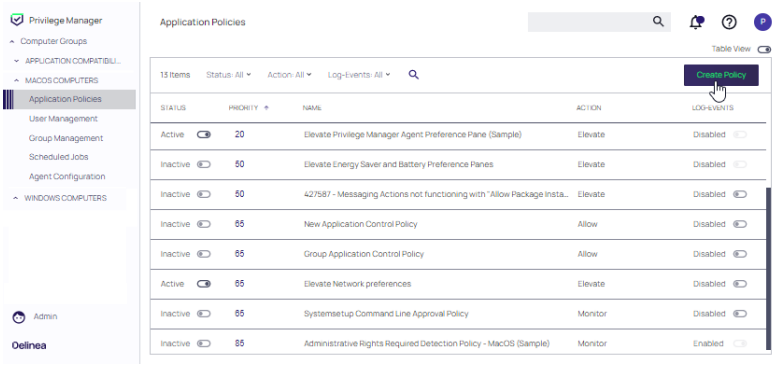


Policy Wizard

The policy wizard provides a guided step-through for the creation of new policies. The policy wizard has variations, depending on your platform and method of policy creation selected.

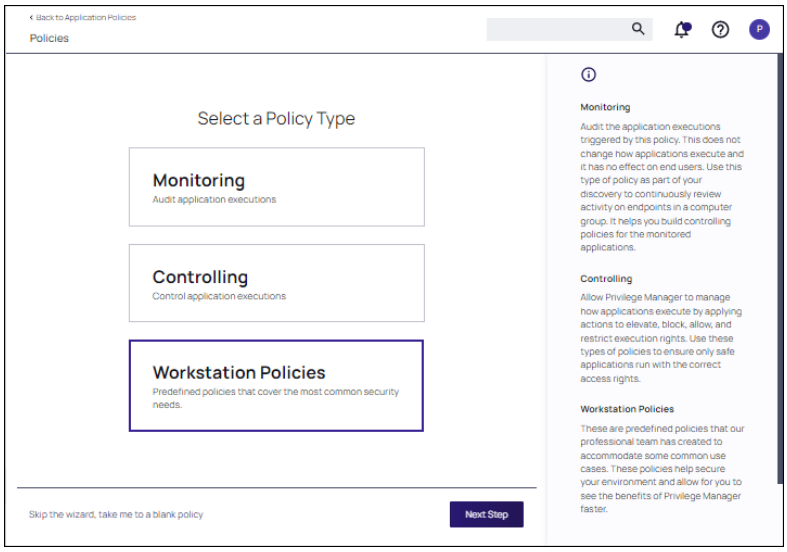
Accessing the Policy Wizard

1. For any of your Computer Groups navigate to **Application Policies** and click **Create Policy**.



2. When the policy wizard is presented, make a selection according to the type of policy you want to create. The policy wizard presents the following methods for creating a policy. Follow each link for instructions.
   - Creating a Monitoring Policy
   - Creating a Controlling Policy

- Creating a Workstation Policy with the Delinea Policy Framework
- Creating a Policy from a Blank Template



Workstation Policies

Workstation policies enable users to implement foundational policies in a Delinea Policy Framework for rapid deployment. For convenience, the following most commonly used policies are available.

Windows Workstation Policies

- **Software Development Tools**

  This high-priority policy targets common software development processes that may run frequently. Targeting them in an early out policy speeds up the policy processing and minimizes delays an end-user could see. This policy will also cause policy evaluation for child processes to be skipped.

- **Visual Studio Installers**

  Silently elevates various Microsoft Visual Studio installers and upgrades, including Visual Studio Enterprise, Community, and Professional.

- **Malware Attack Protection**

  This policy prevents Living Off The Land Binaries (LOLBAS), a cyber attack method that misuses existing legitimate tools or programs on a computer for malicious functions, from being executed by commonly exploited parent applications, such as cmd.exe, bash and PowerShell, among others.

- **Capture Application Elevation Attempts**

  This policy targets non-Microsoft applications that trigger a UAC prompt and sends policy feedback to the server. This policy can be used to learn about applications users attempt to elevate before a silent elevation policy or justification/approval workflow is put into place.

- **Allow Microsoft Signed Security Catalog**

This policy allows Microsoft Signed Security Catalog files (Operating System applications) to run and can be used in combination with blocklist policies to prevent legitimate Operating System Applications from being blocked.

macOS Workstation Policies

- **Elevate Common Preference Panes**

  Silently elevates commonly used preference panes such as the Date and Time, Energy Preferences, and Network Settings.

- **Elevate Xcode**

  Silently elevates Xcode by granting the `system.install.apple-software` and `com.apple.dt.Xcode.LicenseAgreementXPCServiceRights` Authorization rights.

- **Elevate Console**

  Silently elevates the Console application using a just-in-time elevation action limited to 5 minutes. This policy allows a user unfettered Admin access for 5 minutes.

- **Elevate Jamf Commands**

  Elevates the policy and recon Jamf commands after a justification.

- **Elevate Package Installers**

  Silently elevates package (pkg) installers and sends feedback to the server about when this policy is triggered.

- **Elevate sudo pmagentctl updateclientitems**

  Allows all users to run `sudo pmagentctl updateclientitems` without having to input credentials.

- **Block sudo commands for non-admin group users**

  All sudo commands will be blocked unless requested by members of the Admin group. If requested by a member of the Admin group, sudo will resume normal operation.

- **Monitor sudo Usage**

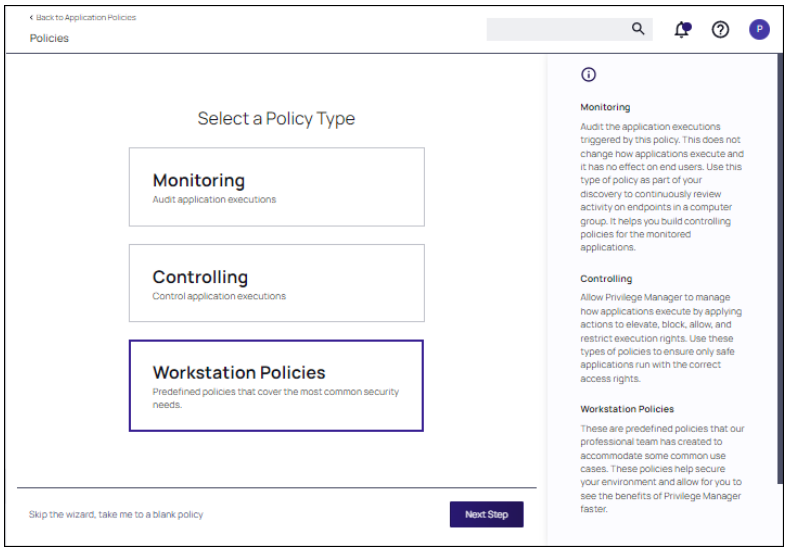
  Monitors the usage of the sudo command and sends feedback to the server.

- **Monitor Admin Applications**

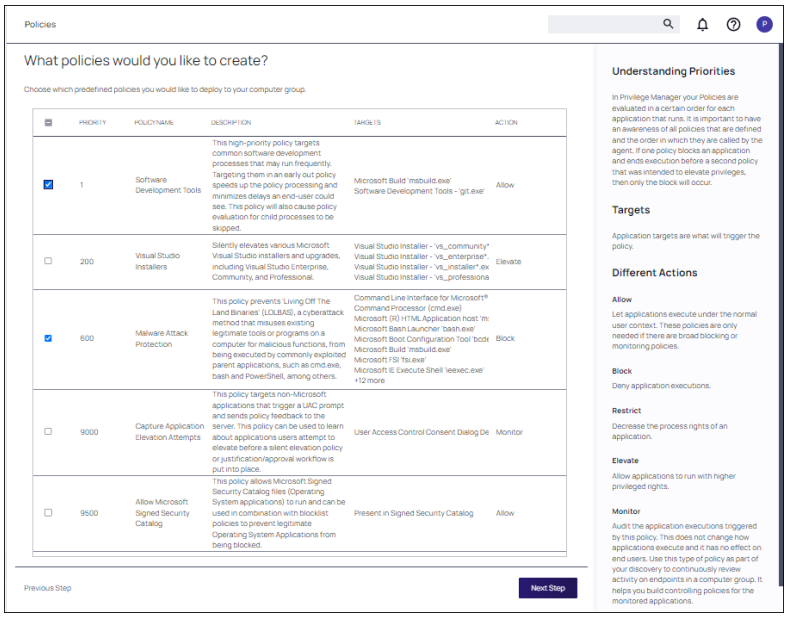
  Monitors for applications launched requiring Admin rights, excluding Apple System applications. This policy can be useful before removing Admin rights from end users.

Creating Workstation Policies

1. Under your Computer Group, navigate to **Application Policies**. Click **Create Policy**.
2. On the **What type of policy?** page, select **Workstation Policies** and click **Next Step**.



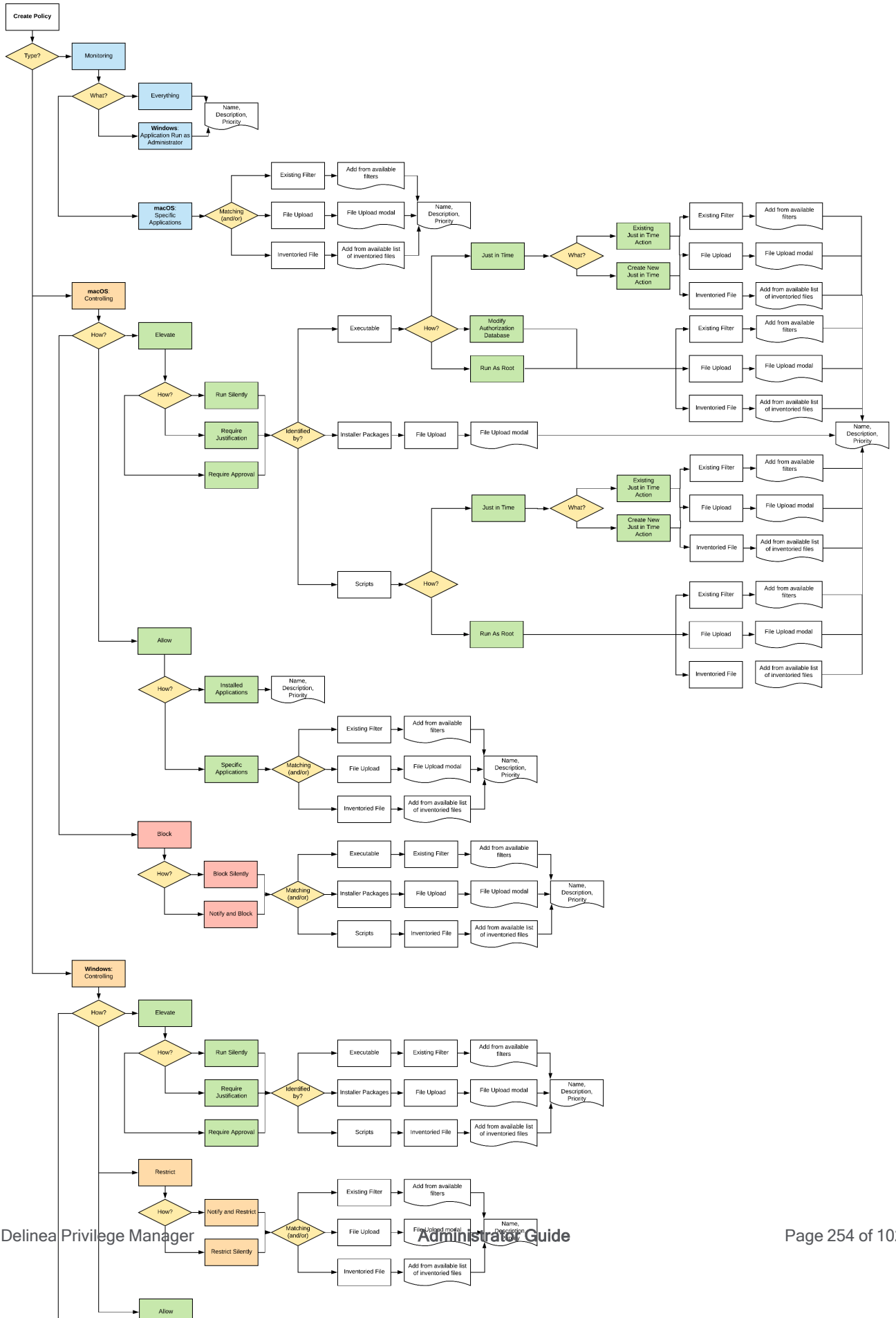
3. On the **What policies would you like to create?** page, select the check box next to the name of the workstation policies to deploy. Note that multiple policies can be selected. Click **Next Step**.



4. Confirm your selections and click **Next Step**. The Application Policies page is redisplayed with the newly added workstation policy.

Full Policy Wizard Diagram

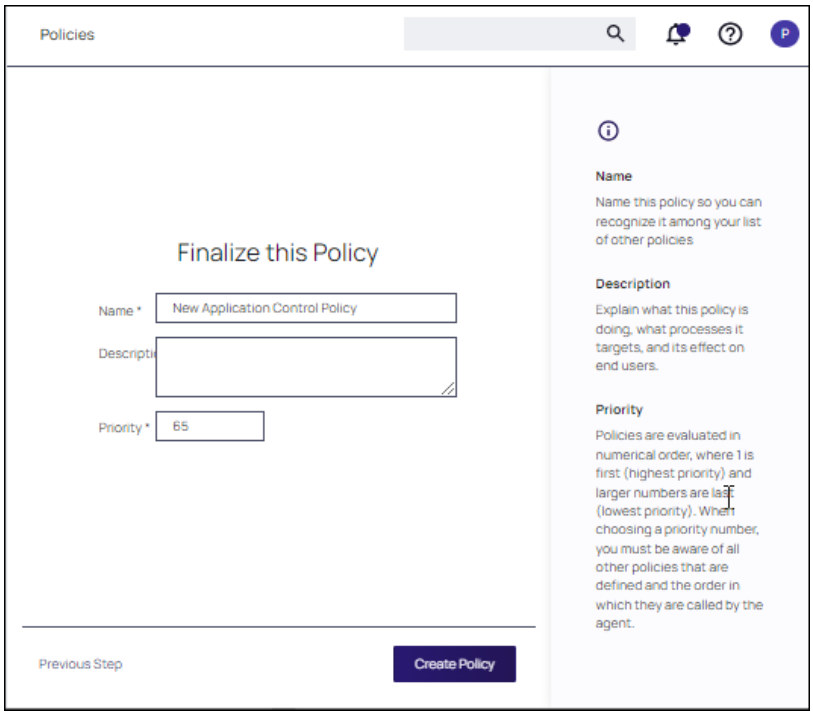
Note: The diagram shows macOS actions "Run as Root" and "Just in Time" which will only work with the system extension based agent introduced with Privilege Manager v10.8.2.


Create Policy
Type?
Monitoring
What?
Everything
Windows: Application Run as Administrator
Name, Description, Priority
macOS: Specific Applications
Matching (and/or)
Existing Filter
Add from available filters
File Upload
File Upload modal
Inventoried File
Add from available list of inventoried files
Just in Time
What?
Existing Just in Time Action
Create New Just in Time Action
macOS: Controlling
How?
Elevate
Executable
Modify Authorization Database
Run As Root
Run Silently
Require Justification
Require Approval
Identified by?
Installer Packages
Scripts
Allow
Installed Applications
Specific Applications
Block
Block Silently
Notify and Block
Windows: Controlling
Restrict
Notify and Restrict
Restrict Silently

Creating a Policy from a Blank Policy

It is possible to create a new policy based on a blank template. On the first page of the Policy Wizard, you can find a link to **Skip the wizard** at the bottom of the page.

Click the link to open a blank policy.

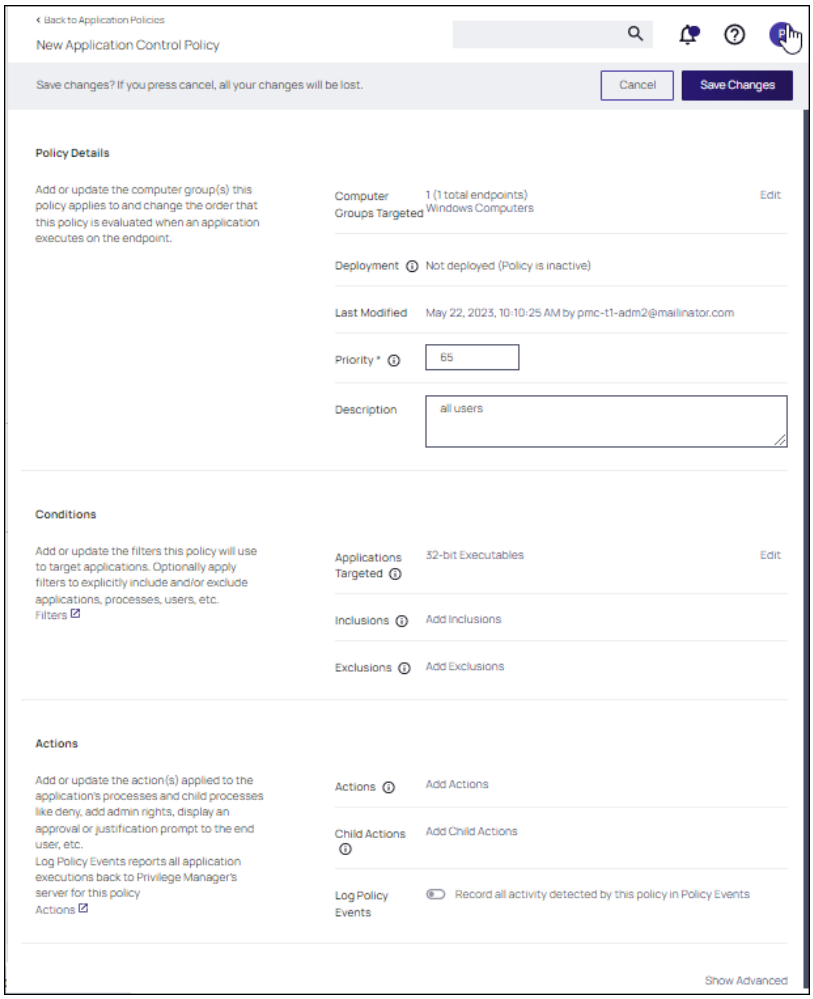


The **General** tab displays. Complete the fields to build the policy out manually. Tool tips are available for field definitions.

Click **Show Advanced** link at the bottom of the page to supply additional parameters for the policy. Ust te toggle at the top of the page to specify if the policy is **Inactive** or **Active**.

Click **Save Changes**.

Computer Groups



Monitoring Policies (Learning Mode)

At the most basic level, a Monitoring policy is a policy that takes no action. It exists only to gather data and you can use the data it gathers for audits or for assigning actions to application events, retrospectively. For trials and Proof of Concept (PoC) environments these can be pointed at specific endpoints in order to learn about events that are already happening, or in order to test-run specific applications that you want to quickly introduce into Privilege Manager.

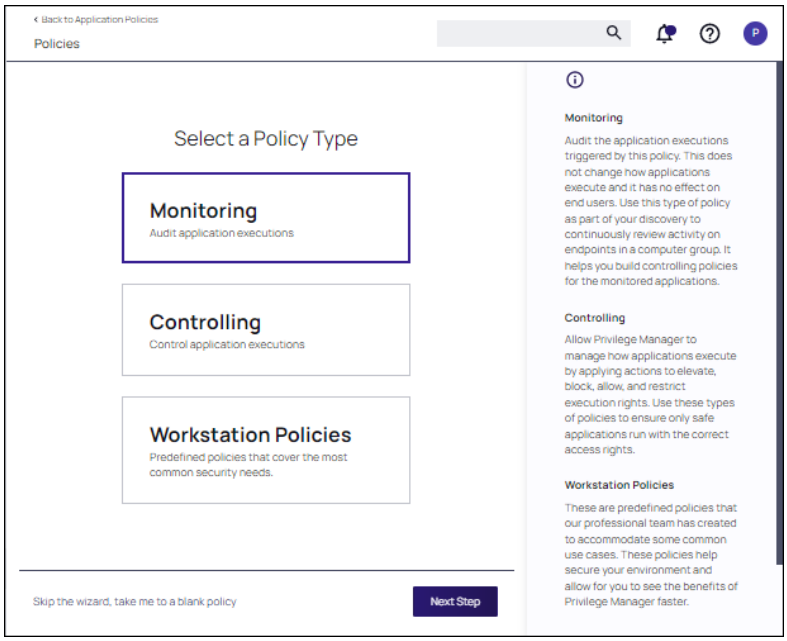
Any Monitoring policy will have the **Audit Policy Events** set to active under the Actions section.

> **Note:** Audit Policy Events is generally inactive in production environments outside of specific auditing or data-collecting initiatives due to the large amount of data these policies can gather.

Creating a Monitoring Policy

Use the policy wizard to create a monitoring policy for the learning mode phase on your instance.

1. Under your Computer Group, navigate to **Application Policies**. Click **Create Policy**.
2. On the **What type of policy?** page, select **Monitoring** and click **Next Step**.



Note: Policies can also be created using a blank policy. Refer to Creating Policies.

3. On the **What processes do you want this policy to monitor in this computer group?** page, select **Everything** and click **Next Step**.
4. Enter a new name for the policy and click **Create Policy**.
5. The policy page is displayed. On the **Settings** tab, continue to customize parameters for the policy, then click **Save**.

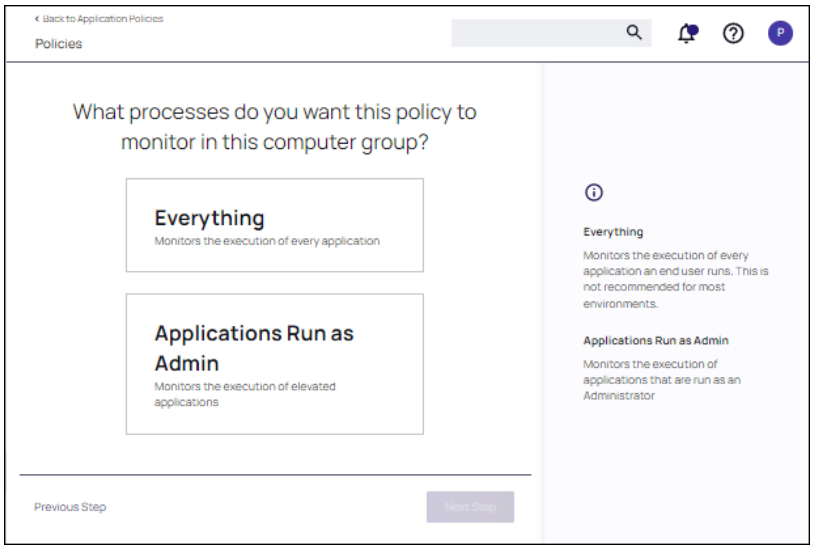
Note: It is not recommended to assign this policy to than a handful of machines.

Discover Applications that Require Administrator Rights

The most influential applications are those that require administrator credentials to run. For setting up endpoints that are organized by Least Privilege, you can use a monitoring policy to discover all events requiring Administrator rights.

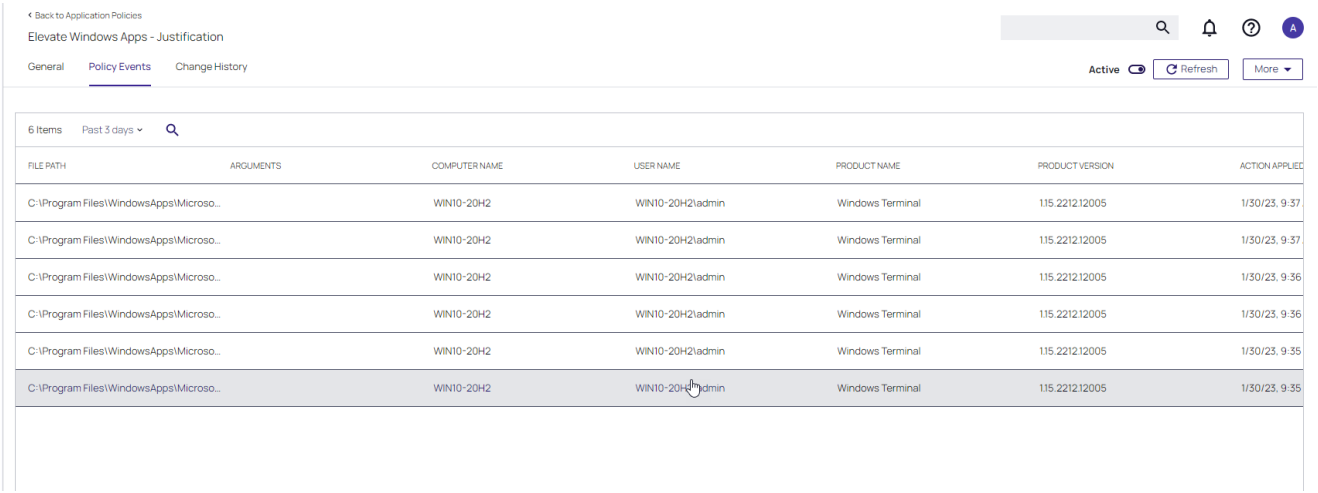
Use the policy wizard to create a monitoring policy for the learning mode phase on your instance.

1. Under your Computer Group, navigate to **Application Policies**. Click **Create Policy**.
2. On the **What type of policy?** page, select **Monitoring** and click **Next Step**.
3. On the **What processes do you want this policy to monitor in this computer group?** page, select **Applications Run as Admin** and click **Next Step**.
4. Enter a new name for the policy and click **Create Policy**.



View Policy Results

To view all feedback, or event, sent from your existing policies with the Send Policy Feedback activity checked, click the **Policy Events** tab for that policy. Events will be listed in the main section and on the left sidebar you can scope results for certain policies, computers, time frame, etc. You can use this view to assign any events to policies by clicking Assign to Policy under the event listing.

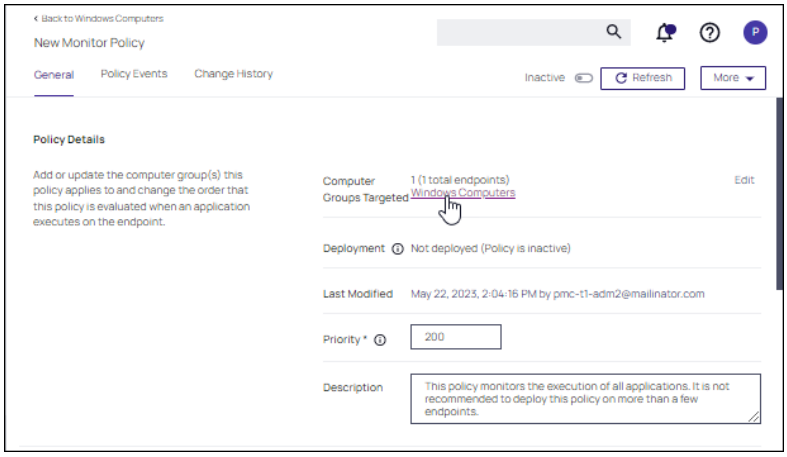


Discover All Events on Test Workstations

Another type of monitoring policy will discover all events on targeted machines regardless of whether the application requires Administrator Rights. This policy is used in test environments to quickly target policies at untrusted/unwanted applications, but is not recommended for production settings.

1. Under your Computer Group, navigate to **Application Policies**. Click **Create Policy**.
2. On the **What type of policy?** page, select **Monitoring** and click **Next Step**.

3. On the **What processes do you want this policy to monitor in this computer group?** page, select **Everything** and click **Next Step**.
4. Enter a new name for the policy and click **Create Policy**.
5. In the **General** tab, locate **Computer Groups Targeted**.



6. Add the **Application Compatibility Testing Windows Computers (Target)** collection and remove the **Windows Computer** target.
7. Click **Update**.

Controlling Policies

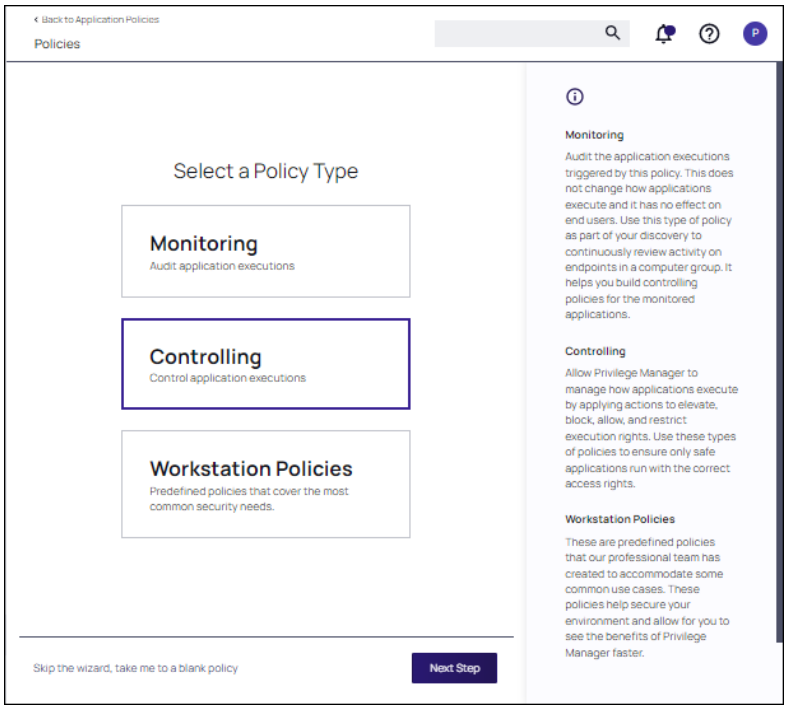
The following diagrams demonstrate the decision points you will step through in the wizard for a controlling policy.

- macOS
  - Controlling Allow Diagram
  - Controlling Block Diagram
  - Controlling Elevate Diagram
- Unix/Linux
  - "Unix/Linux Specific Policies" on page 398
- Windows
  - Controlling Allow Diagram
  - Controlling Block Diagram
  - Controlling Elevate Diagram
  - Controlling Restrict Diagram

Creating a Controlling Policy

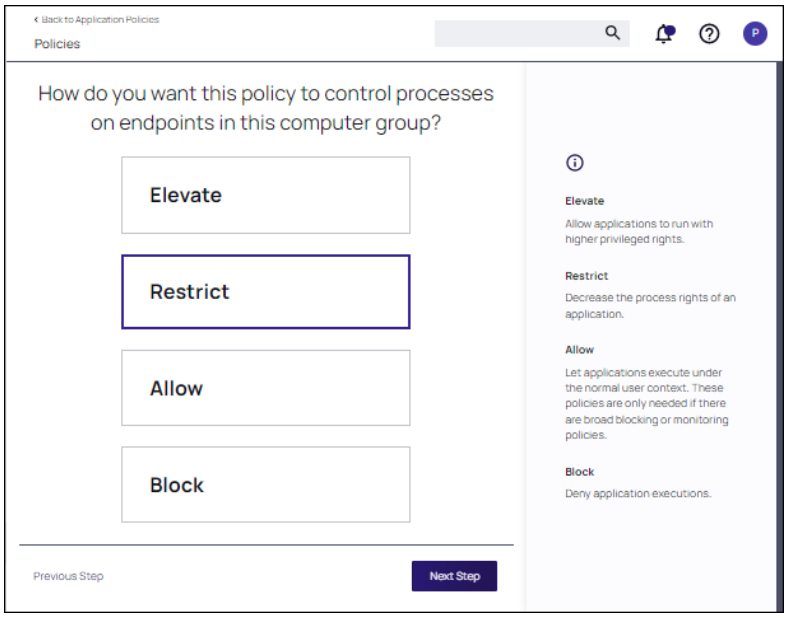
Use the policy wizard to create a controlling policy to control processes on for your instance.

1. Under your Computer Group, navigate to **Application Policies**. Click **Create Policy**.
2. On the **What type of policy?** page, select **Controlling** and click **Next Step**.



Note: Policies can also be created using a blank policy. Refer to Creating Policies.

3. On the **How do you want this policy to control processes on endpoints in this computer group?** page, select the type of control (**Elevate**,**Restrict**,**Allow**,**Block**) and click **Next Step**.



4. The next steps allow you to specify processing options that are dependent on the process selected.
   - Elevate: run elevated processes silently, require justification or approval
   - Restrict: restrict silently or notify an restrict
   - Allow: allow execution of operating system files or specific applications
   - Block: block silently or notify an block

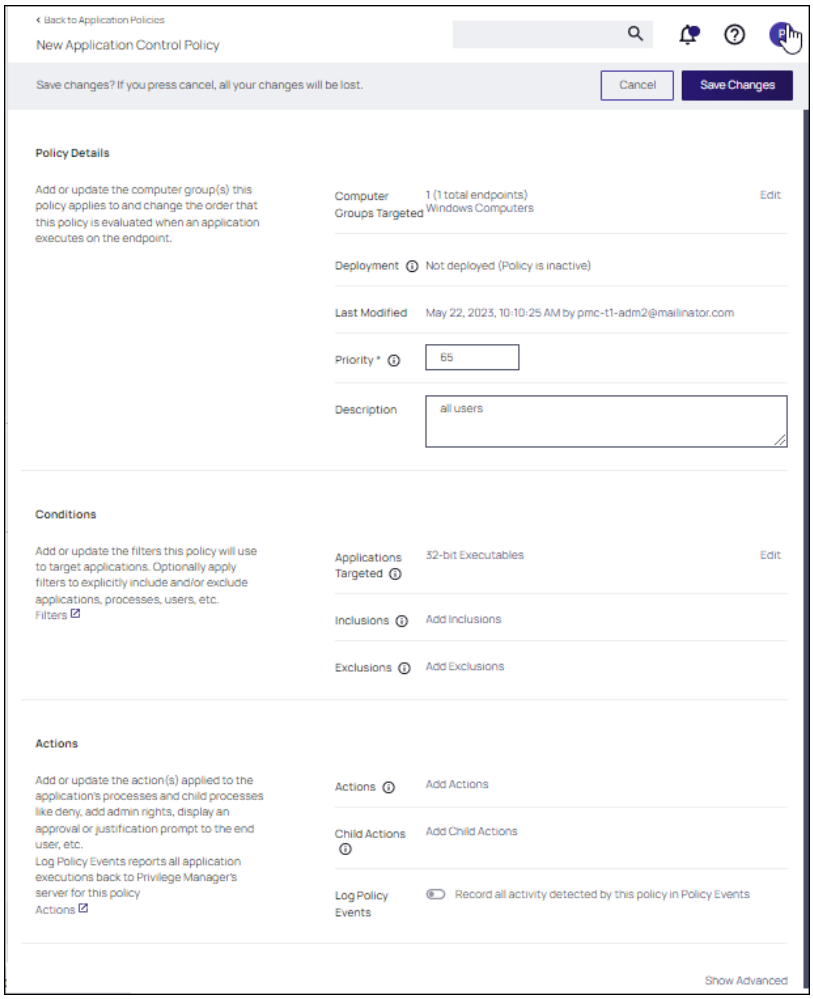
   Make this appropriate selection and click **Next Step**.
5. Enter a new name for the policy and click **Create Policy**.
6. The policy page is displayed. On the **Settings** tab, continue to customize parameters for the policy, then click **Save**.

Activating and Customizing a Policy

Once a policy is created, it can be customized. The following screen capture shows a policy example that denies the execution of a specific batch file.

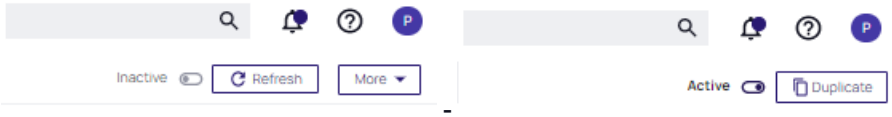
Note: If you need to modify any items within Privilege Manager, duplicate the item and modify the duplicate instead of the built-in item so that an upgrade does not overwrite it.

Computer Groups



Policy Activation

By default newly created policies are inactive and to activate them, the switch needs to be set to active.



Policy Details

The Policy Details section provides information about and customization options for:

- **Computer Groups Targeted** can be edited by either
  - deleting the current target by clicking the **x** next to the computer group name, or
  - adding another computer group by clicking **Add**.

- **Deployment**, provides information about the deployment status at endpoints. Click the explanation point next to Deployment to run the **Resource and Collection Targeting Update Task**.
- **Last Modified** provided a quick history on the last edit to the policy, time and by whom.
- **Priority**, modify the priority if needed, specific deny policies get lower priority values than monitor, allow, or elevate policies.

Conditions

Under Conditions edit the

- Applications Targeted,
- Inclusions, and
- Exclusions.

Actions

Under Actions edit which message action to use, if child actions are applicable, and if you wish to audit all activities this policy is detecting.

- Actions
- Add Child Actions
- Audit Policy Events

Audit Policy Events

All activity identified on a policy can be recorded by using the Audit Policy Events switch. This setting is automatically enabled for all monitoring policies. It can be activated on demand for controlling policies. Once selected, a confirmation message appears advising users that this functionality should only be enabled for a limited time on a selected number of endpoints.

> **Note:** For Unix/Linux endpoints the `pmagent --privman --refreshpolicies` command needs to run, to update the policy on the endpoint.

Show Advanced

Clicking **Show Advanced**, provides access to setting Policy Enforcement options, like:

- Continue Enforcing
- Applies to All Processes
- Enforce Child Processes
- Stage 2 Processing
- Skip Policy Analysis at Start-up.

Refer to Policy Enforcement for further details.

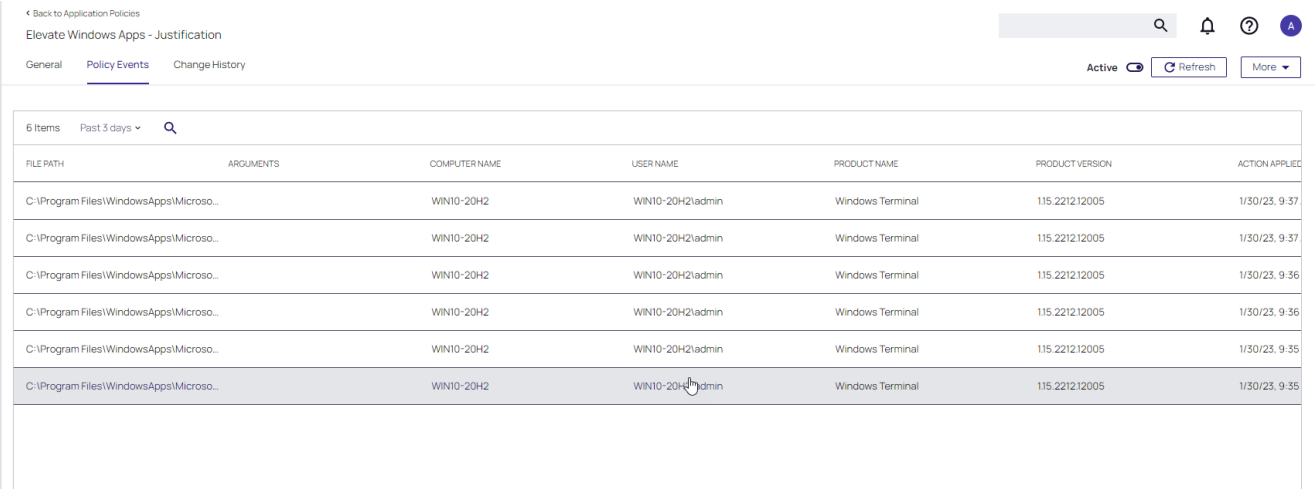
Policy Events Tab

The Policy Events tab lists all events that were discovered with this specific policy.

The Policy Events page provides the

- File Path
- Computer Name
- User Name
- Product Name
- Product Version
- Action Applied
- Command Line

information for the active application control policy creating the events.



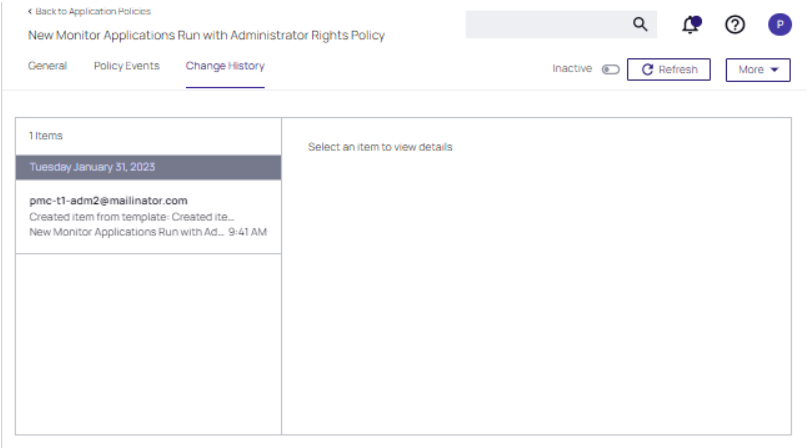
Unix/Linux Policy Events Tab

The Policy Events page for Unix/Linux shows a subset of the information available for macOS/Windows systems on this page.

Change History Tab

The Change History tab provides insight into any change events for the specific policy.

Computer Groups



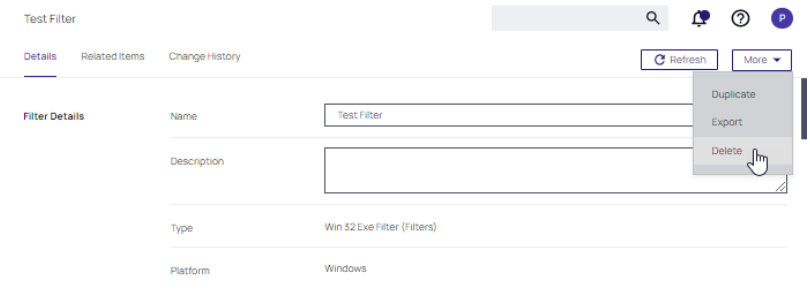
Deleting Items

When deleting items, there might be dependencies, like a filter that is used in a policy. If that filter is deleted without modifying or deleting the policy, the policy will stop working without anyone realizing that the filter has been deleted.

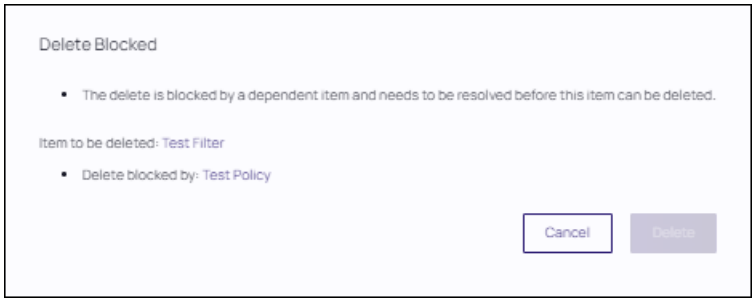
Privilege Manager detects dependencies when items are deleted and alerts the user to:

- any dependent items, which block the deletion.
- any child items, which will also be deleted.

Select **Delete** from the **More** pull-down.



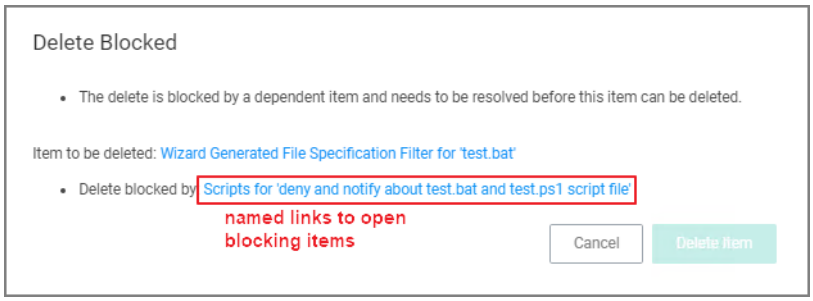
If that filter is part of a policy and **Delete** is selected, the **Item Dependency: Delete Blocked** modal opens.



From the modal, the user can see that the delete is blocked by a dependent item.

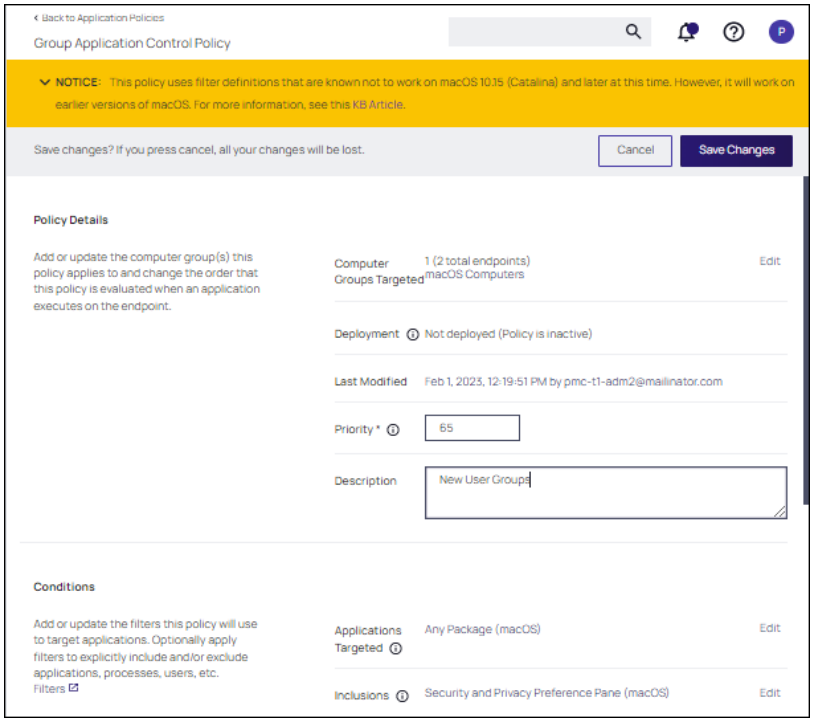
While there are blocking items, **Delete** or **Delete Item and Children** are disabled. Delete is dynamic and will only display **Delete Item and Children** if both of those are dependencies, otherwise it will only display **Delete**.

Blocking dependent items can be accessed and deleted by clicking on the named item link. This opens the dependent item in another browser tab, where it can be viewed and deleted. For example:



Warning Banner indicating Filter Error Conditions in Policies

A warning banner on the top of a policy page indicates error conditions in the policy due to conflicting filters or OS version based restrictions/limitation for an applied filter.



The warning banner in the image indicates that the filter selected as an inclusion filter does not work with macOS 10.15 or later versions.

The banner is displayed for the following conditions:

- A filter has a warning banner associated due to targeting a macOS preference pane in combination with a conflicting computer group.

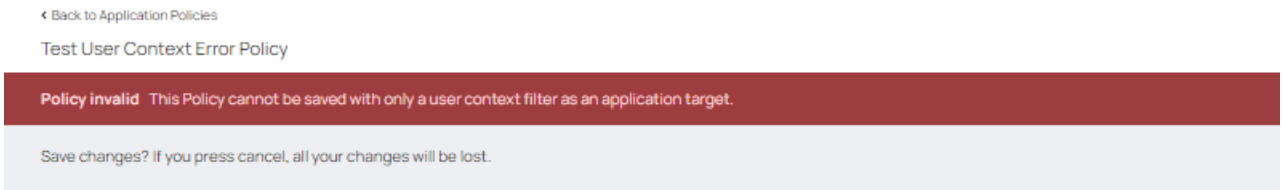
- A filter starts with `com.apple.preference` or the file path starts with `/System/Library/PreferencePanes/`.
- Invalid filter definitions are selected.

The banner is expandable and lists all filter definitions creating the potential conflict. Each filter definition is a hyperlink to the offending filter.

Removing the offending filters from the policy clears the banner warning.

Invalid Policies

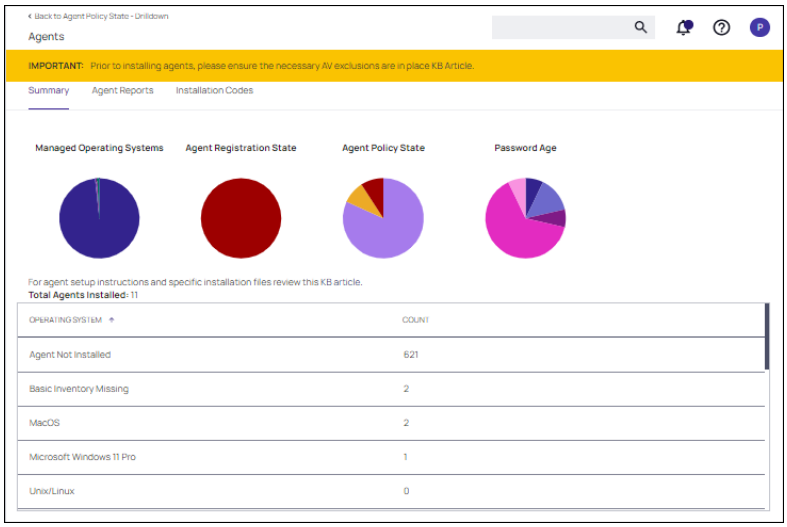
When a policy has a user context filter as the only application target, the policy validation fails and a **Policy invalid** warning is displayed.



Agent Policy State

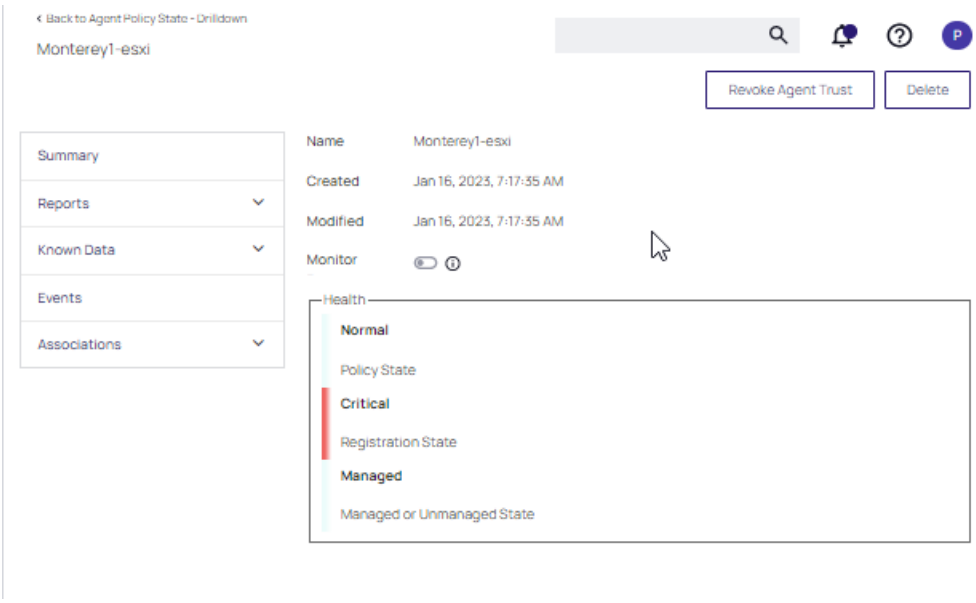
These are the steps for verifying which policies were received by an agent:

1. Navigate to **Admin | Agents** and click on **Agent Policy State**.

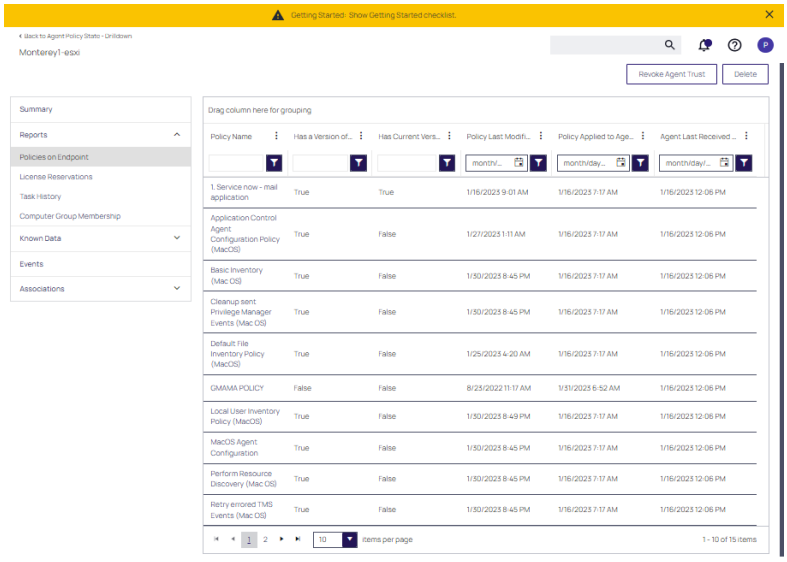


2. On the **Agent Policy State - Drilldown** page select the computer, whose policy state you wish to examine.
3. This opens the Resource Explorer for the selected endpoint.

   Revoke Agent Trust is available, if needed. It removes the agent registration record, which includes the security certificate used to register. The agent will not be able to re-register, update policies, or send events unless it's given a valid install code.



4. Open the **Reports** section and select **Policies on Endpoint**.

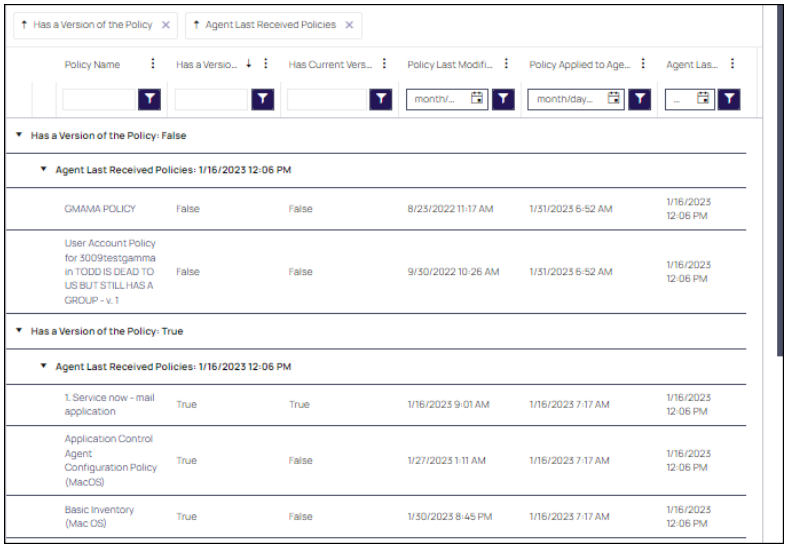


View the polices that the agent on the endpoint has received. The Filter on each column allows you to search for specific policies. The paging controls at the bottom of the page, along with the **items per page** setting control the display of endpoints in the table.

The column details are:

- **Has a Version of the Policy** and **Has Current Version of the Policy** provide information about the version of the policy.
- **Policy Last Modified** informs when a policy was last changed.
- **Policy Applied to Agent** specifies when the policy was first received by the agent.
- **Agent Last Received Policies** informs when the agent last contacted the server to request updates.

5. You can also group the endpoints by levels and sublevels by dragging columns in the area labeled **Drag column here for grouping**. In this example the endpoints are sorted whether or not the endpoint has a version of the policy (**Has a Version of the Policy**) and if so, when the policy was last received (**Agent Last Received Policies**).



Policy Priority

In Privilege Manager your Policies are evaluated in a certain order for each application that runs. It is important to have an awareness of all policies that are defined and the order in which they are called by the agent. If one policy blocks an application and ends execution before a second policy that was intended to elevate privileges, then only the block will occur.

The Policy Priority setting can be found on the Policies main screen in the left column. By default, policies are ordered according to their priority. You can edit this setting under the General tab after clicking into a policy.

Why Policy Priority Matters

To illustrate the way policies are applied in order, this use case will define two policies to

- block MMC.EXE, but
- allow a specific MMC Snap-in.

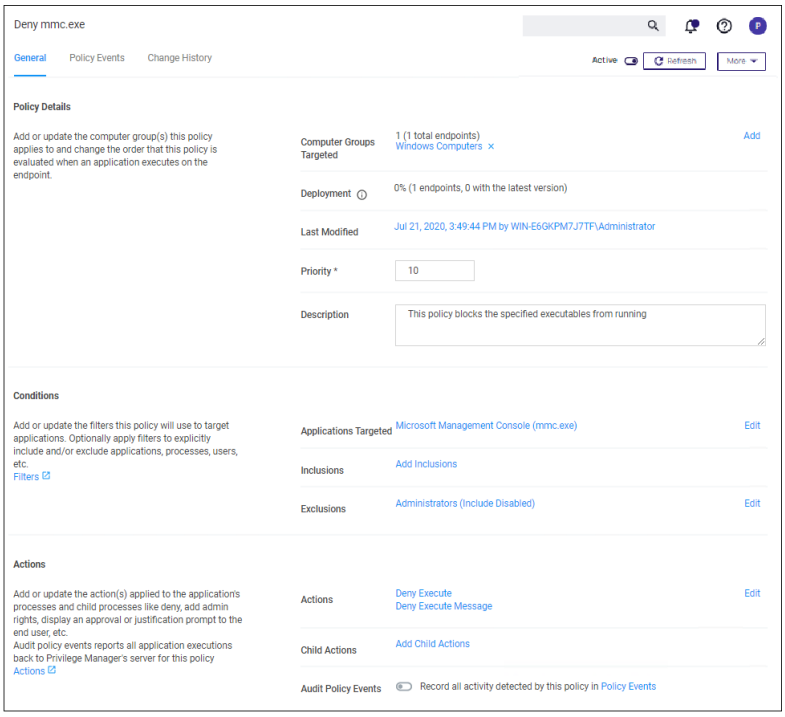
Deny MMC.EXE Policy setup

1. We will create a policy at with a default priority level of 10. This policy will block the execution of MMC.EXE.

   Privilege Manager provides a filter to identify the executable mmc.exe. This can be used in this policy to block mmc.exe. Search for mmc.exe from the main screen search tool. Select the filter named Microsoft Management Console (mmc.exe). Review how the Filter is setup. Note that both File Name and File Path parameters are used.

2. Create the deny mmc.exe policy.

a. Under your **Computer Group** select **Application Policies**.
b. Click **Create Policy**.
c. Select **Controlling** and click **Next Step**.
d. Select **Block** and click **Next Step**.
e. Select **Block Silently** and click **Next Step**.
f. Select **Executables** and click **Next Step**.
g. Select **Existing Filter**.
h. Search for **mmc.exe**.
i. Next to **Microsoft Management Console (mmc.exe)** click Add.
j. Click **Update**.
k. Click **Next Step**.
l. Set the **Inactive** switch to **Active**.
m. Click **Add Exclusion** to set an exception filter to not have this policy apply to Administrators.
n. Search for the **Administrators (Include Disabled)** filter.
o. Click **Add**.
p. Click **Update**
q. Click **Save Changes**.



The policy will now be listed on the Application Policies page under the deny group. Once the policy is delivered to the endpoint agent, mmc.exe will be denied execution for all users without administrator credentials on all target computers. See details on how to deliver policies to the endpoint in the Sending Policies to Endpoints topic.

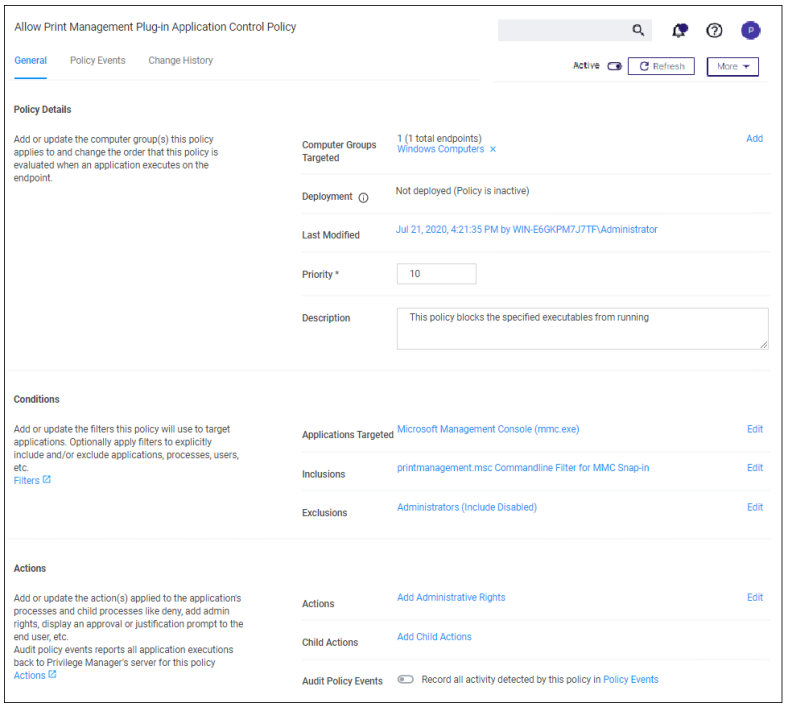
Once the policy is delivered to the endpoint, test running mmc.exe to see the results.

Allow specific MMC Snap-in

Next, we will create a policy that has a priority of less than 50 and it will allow specific MMC snap-ins. Having a priority less than 50 means this policy will be examined before the Deny MMC Console Application Control Policy.

1. As a short cut to this use case, start by duplicating the policy we just created, select **More | Duplicate**
2. Name the new policy Allow Print Management Plug-in Application Control Policy.
3. Click **Create**
4. Set the **Policy Priority** value to 9. (This level is not required, only defined for this use case.) This means that this policy will be examined prior to the policy that blocks the mmc console. If the conditions are met, printmanagement.msc will run with elevation.
5. Under **Conditions**, click **Add Inclusions** and search for the **printmanagement.msc Commandline Filter**.
6. Click **Add**.
7. Click **Update**. This filter will identify the mmc.exe file ONLY if the printmanagement.msc is run.
8. Under **Actions**, click **Edit**.
9. Next to **Deny Execute** and **Deny Execute Message**, click **Remove**.
10. Search for **Add Administrative Rights**, click **Add**.
11. Click **Update**.
12. Click **Save Changes**. You will now see your two policies in your Policies List. Once this policy is delivered to the

endpoint agent, printmanagement.msc will be elevated with administrative rights.

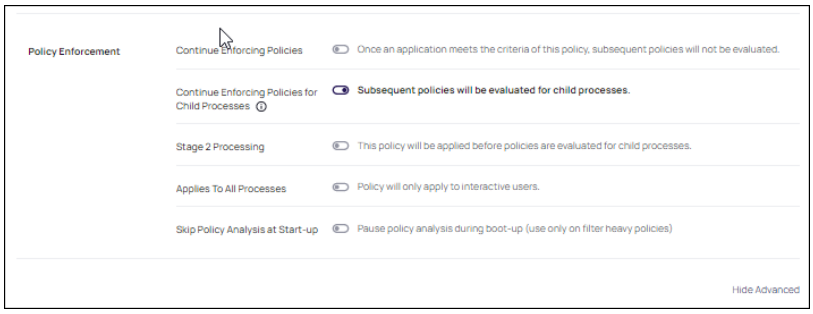


Test this use case

1. Run MMC.EXE from an endpoint where the user is NOT an administrator. This MMC.EXE execution will be denied execution.
2. Run printmanagement.msc from an endpoint where the user is NOT an administrator. This MMC snap-in will run with elevation.
3. Change the Policy Priority of your “Allow Print Management Plug-in Application Control Policy” to Priority 11 rather than priority 9. Repeat the second test. When you now run printmanagement.msc, the application will be blocked despite your elevation policy. This is why it is crucial to keep the priority levels that are set for your policies in mind and adjust them to meet your intended system requirements.

Policy Enforcement

Each policy has advanced settings to address any non default Policy Enforcement options. Some of those pertain to parent-child processes and how policies are processed when they are supposed to work together in such parent-child or stage 2 processing scenarios.



Continue Enforcing

After an application meets the criteria of this policy, the agent will continue checking if it matches additional policies. If this setting is not enabled, subsequent policies will not be evaluated.

This setting has to be active for **Stage 2 Processing** to work as intended.

Continue Enforcing Policies for Child Processes

Include child processes in the policy enforcement, meaning subsequent policies will be evaluated.

In certain situations this needs to be disabled, if for example you want to allow and application if it is launched by a specific process, but deny it if it's executed directly. Refer to the **Stage 2 Processing** description.

Stage 2 Processing

Policies are initially evaluated for the primary process. If no matches are found, policies are evaluated for a parent of that process. If active, the policy is applied before policies are evaluated for child processes.

For example, if you want to allow regedit.exe when launched by cmd.exe but block it if launched directly, you need to create

1. a policy to target and allow cmd.exe with an inactive "Enforce Child Processes" and
2. a policy that targets regedit.exe with a deny action and "Stage 2 processing" enabled.

The priority on the policy that targets regedit.exe directly needs to be higher than the priority on the allow cmd.exe policy.

Applies to All Processes

Policy will apply to system based processes. If this setting is not active, the policy will only apply to interactive users.

Skip Policy Analysis at Start-up

This setting can be used to pause policy analysis during boot-up, refer to Increase Boot-up Performance for details.

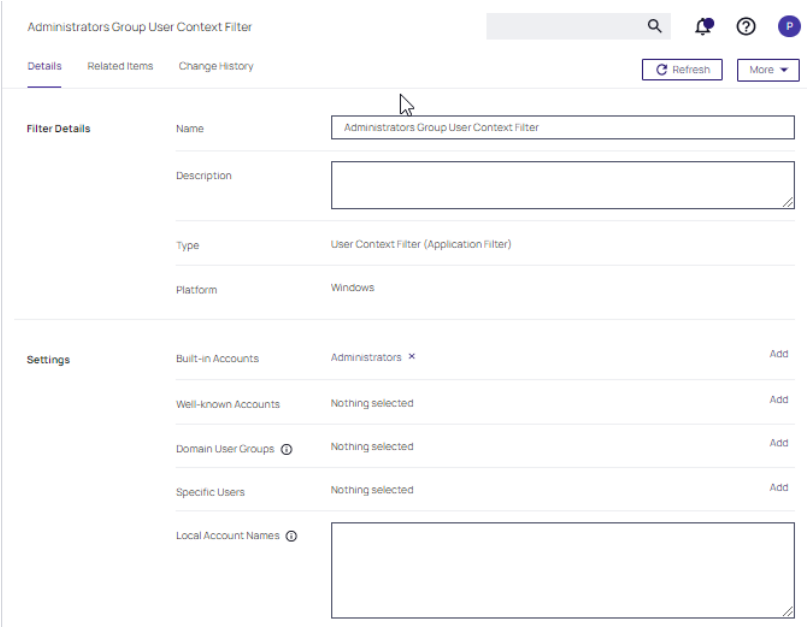
Exclusion of Users on Policies

If you wish to exclude certain users with a filter from an application policy, follow these general guidelines.

Targeting Administrators with the Exclusion

To target the Administrators group, you need to use a User Context filter and select **Administrators** for the **Built-in Accounts**. The out-of-the-box **Administrators (Include Disabled)** filter (item f9569529-62d4-49ba-aa21-b9362e1f4de6) accomplishes the same. Include disabled text just means the user is a member of the group, but the process may or may not be elevated.

This is an example of a working filter for the Administrators Group:

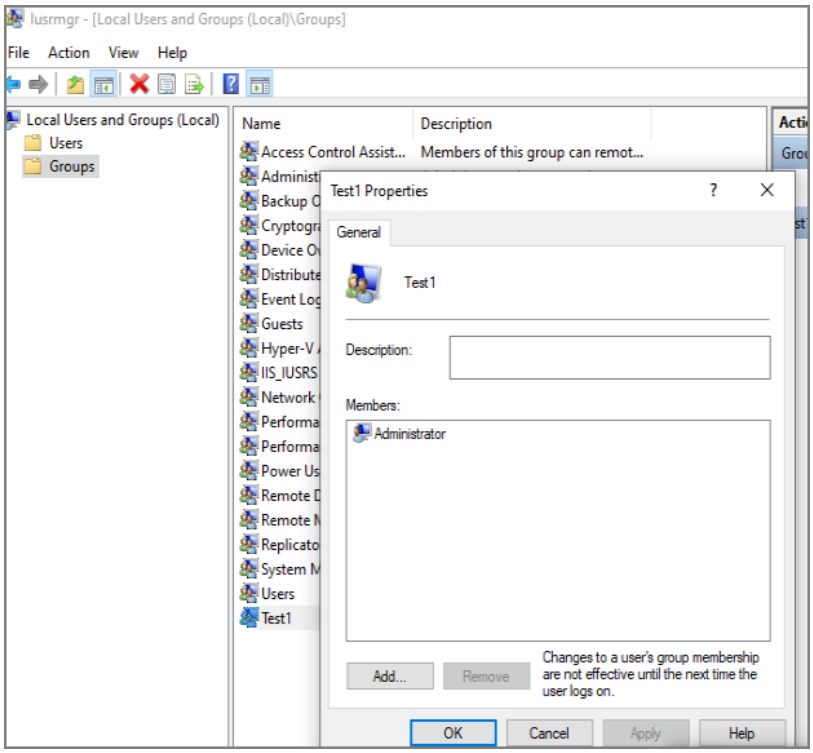


Targeting new Local Groups (not built-in)

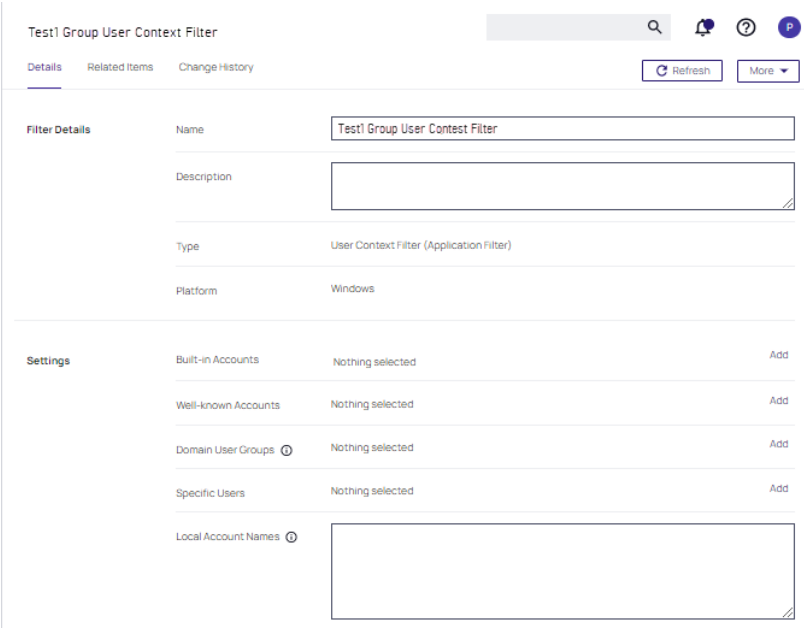
The **Local Group Names** option can be used to target new local groups. New local groups are user groups that are not considered built-in system or out-of-the-box Windows groups, such as Users, Administrators, Power Users, Backup Users, etc.

For example, create a new local group on a local computer and call the group "Test1". Then add a user to it that you wish to exclude.

Computer Groups



In this example, if you configure a filter like this, the following policy should correctly exclude users in the group.



Using RegEx in Policies and Filters

Various Privilege Manager policies and filters use Regular Expressions (RegEx) to specify application or file names to match against.

For Privilege Manager all RegEx strings need to be in lowercase. A good resource for testing RegEx is https://regexr.com

Special RegEx Characters

The following characters have special meaning in RegEx, and should be used with an escape character when there is a need to represent a literal character.

To perform the escape a \ (backslash) needs to precede the following characters: `+ * ? ^ $ . [ ] { } ( ) | \ /`

A Privilege Manager Win32 file filters path name does not use the ending directory slash \. RegEx for path names should also not include the ending \.

Escape Example

For the literal `(x86)\.net\C++` the RegEx is `\(x86\)\\\.net\\c\+\+`.

Wildcard Example

In RegEx: `.*` is a wildcard

File Name Examples

Match with Wildcard before the File Name

Matching anything before the file name and ending with a file type, use a wildcard before the file name.

`File Name="*eetechcode.exe"` use this in Privilege Manager`(.*eetechcode\.exe$)`

Results:

- Match eetechcode.exe
- NoMatch eetecTesThcode.exe
- NoMatch eetechcodeTesT.exe
- Match TesTeetechcode.exe

Match File Name Containing String and File Type

To match a filename that contains a character string on both sides of the actual file name and that must end with a specific file type:

`File Name="*eetechcode*.exe"` use this in Privilege Manager`(.*eetechcode.*\.exe$)`

Results:

- Match eetechcode.exe
- NoMatch eetecTesThcode.exe
- Match eetechcodeTesT.exe
- Match TesTeetechcode.exe

Match with Wildcard at end of File Name and before File Type

Matching a file name with a string that contains anything between the string and the file type.

`File Name="eetechcode*.exe"` use this in Privilege Manager`(^eetechcode.*\.exe$)` this is a

Results:

- Match eetechcode.exe
- NoMatch eetecTesThcode.exe
- Match eetechcodeTesT.exe
- NoMatch TesTeetechcode.exe

Match with Wildcard in the Middle of Two Strings

Matching a file name beginning with a sting, followed by a wildcard and another string with the last string that includes the file type at the end.

`File Name="eetech*code.exe"` use this in Privilege Manager`(^eetech.*code\.exe$)`

Results:

- Match eetechcode.exe
- Match eetecTesThcode.exe
- NoMatch eetechcodeTesT.exe
- NoMatch TesTeetechcode.exe

Match with Wildcard at End of File Type

Matching a file name with the wildcard at the end of the file name after the file type, when the filename begins with a string that includes the file type and matches anything after the file type.

`File Name="eetechcode.exe*"` use this `(^eetechcode\.exe.*)`

Results:

- Match eetechcode.exe
- NoMatch eetecTesThcode.exe
- NoMatch eetechcodeTesT.exe
- NoMatch TesTeetechcode.exe

File Path Examples

Wildcard at the End of the Path

To match when a wildcard is at the end of the File Path like:

`File Path="C:\Program Files\Thycotic\Agents\Agent\*"` use this `(^c:\\program files\\thycotic\\agents\\agent.*)`

Note: The final backslash has been removed for Privilege Manager.

Also note the system variables like `%ProgramFiles%` don't work using regex unless `%ProgramFiles%` is what is shown in the Privilege Manager logs for the event.

Results:

- Match C:\Program Files\Thycotic\Agents\Agent
- NoMatch \Program Files\Thycotic\Agents\Agent
- NoMatch %ProgramFiles%\Program Files\Thycotic\Agents\Agent
- Match C:\Program Files\Thycotic\Agents\Agent\x86

Wildcard in IP Address for Network File Path

To match when a wildcard is used in an IP address for a network File Path like:

`File Path="\\10.10.10.*\Program Files\Thycotic\Agents\Agent"` use this
`(^\\\\10\.10\.10\..*\\program files\\thycotic\\agents\\agent$)`

Note: The final backslash has been removed for Privilege Manager.

Results:

- No Match C:\Program Files\Thycotic\Agents\Agent
- NoMatch \Program Files\Thycotic\Agents\Agent
- NoMatch %ProgramFiles%\Program Files\Thycotic\Agents\Agent
- NoMatch C:\Program Files\Thycotic\Agents\Agent\x86
- Match \10.10.10.2\ProgramFiles\Thycotic\Agents\Agent
- Match \10.10.10.9\ProgramFiles\Thycotic\Agents\Agent

Wildcard for Application Updates for all Users

To match when a wildcard is used several times to target application updates for all Users:

`File Path "*\Users\*\AppData\Local\Temp\notepad++\*\bin"` use this
`(.*\\users\\.*\\appdata\\local\\temp\\notepad\+\+\\.*\\bin$)`

This targets any drive, any user, and multiple versions of an application update. Building filters like these can help streamline Privilege Manager administration since the filter stays current even with new versions coming out and working for all users.

Results:

- Match C:\Users\MarkH\AppData\Local\Temp\notepad++\1.23.59874\bin
- Match C:\Users\DarinS\AppData\Local\Temp\notepad++\1.23.59874\bin
- Match C:\Users\MarkH\AppData\Local\Temp\notepad++\2.56.89457\bin
- Match C:\Users\DarinS\AppData\Local\Temp\notepad++\2.56.89457\bin
- NoMatch C:\Users\MarkH\AppData\Local\Temp\notepad++\2.56.89457
- NoMatch C:\Users\MarkH\AppData\Local\Temp\notepad++\2.56.89457\bin\test

Example Policies

This sections contains examples on how to configure and use policies in Privilege Manager.

These following topics are available:

- Approval Policies
  - Offline Approvals
  - HelpDesk Approvals
  - Setup a Policy to use Google Authenticator
- Allow Policies
  - Google Application with File Upload
  - Microsoft Security Catalog
- Elevation Policies
  - UAC Override Policy
  - Elevate Applications launched from Network Share Policy
  - Elevate msi launched from a Network Share
  - Elevate Applications whose Execution Requires Approval
  - Elevate Applications that Require User Justification
  - MS Visual Studio Installations - Filters and policy now provided via Configuration Feeds. Refer to Config Feeds for download and installation information.
- Monitoring Policies
  - Using a Catch All Policy
  - Reputation Checking Policies
- Blocking Policies
  - Blocking Specific Applications
  - iTunes with File Upload
  - Quarantine Specific Malware
  - Catch-all Blocking Policy
- macOS Specific Policies
  - Allow Copy/Install of Applications
  - Application Self-elevation
  - Require Justification for Firefox
  - Deny Photos Application
  - Adding macOS Agents to a Computer Testing Group
  - Inventorying .pkg Files

Approval Policies

Approval policies require an end-user justification and use an admin approval workflow.

This policy type requires that people provide a justification for why they need to run an application before elevating with administrator privileges. User Justification refers to the policy action. Since Conditions and Actions are independent, this action can be applied to any condition.

The following examples are available:

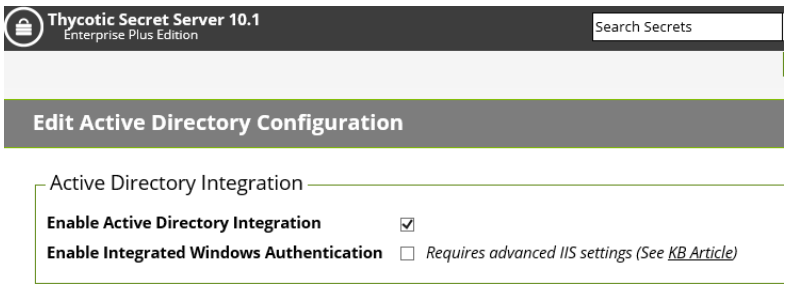
- Offline Approvals
- HelpDesk Approvals
- Google Authenticator approval
- macOS Approval Process

Google Authenticator

This topic describes how to set up a Privilege Manager policy for enabling two-factor functionality with Google Authenticator.

Follow the steps described below to set up a policy for enabling two-factor functionality with Google Authenticator.

1. If you are using the Secret Server login for Privilege Manager, make sure you log in with an Active Directory credential. If you are currently using a Secret Server credential, you need to enable Active Directory Integration.



1. Once you log in with an Active Directory credential go to this URL:

   https://[ServerName]/Tms/Account/Totp

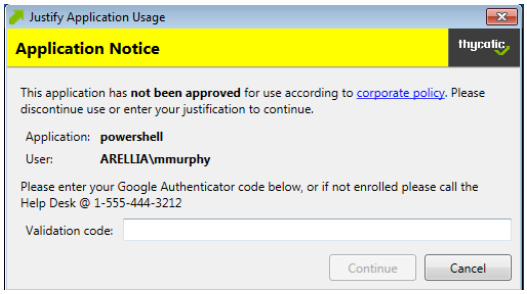
2. There you will see the QR Code or Secret to input into Google Authenticator in order for your user account to authenticate on the endpoint. Each user will need to go to this URL after logging in to Secret Server and add this QR Code to their authenticator app. Users can NOT re-use the same authenticator code that they are using for Secret Server.
3. After you have done that with one of your user accounts, you need to import an XML file as follows:
   a. Access the topic, XML for Challenge Response Message Actions. It contains XML code, copy all that XML code.
   b. Go to https://[ServerName]/Tms/PrivilegeManager/#/item/xml/

c. Paste the contents of the XML code (which you copied in a previous sub-step) into the text field and click the Import button.

4. You can then go to each policy for which you want to enable the two-factor prompt and add the "Challenge/Response Message Action" as an action.

   Note: It is not recommended that you do this for ALL applications that are being run.

5. The end users will then see a prompt such as shown below, when they go to launch an application which triggers that action:



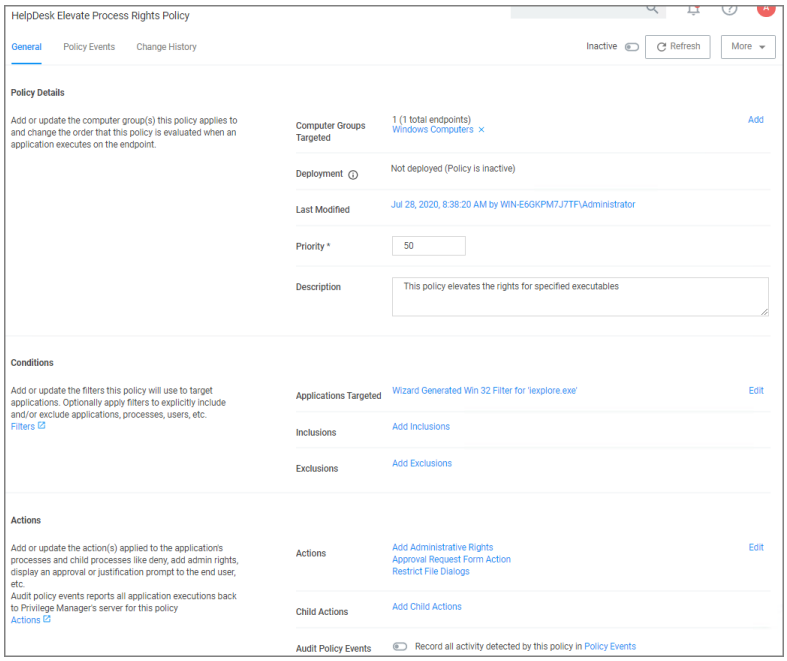
Note: Justification prompt messages are customizable.

Help Desk Approvals

Privilege Manager enables end users to request elevation and then have their request approved or denied by the helpdesk. You can approve or deny requests via the Privilege Manager console, or forward requests to a third-party ticketing system such as ServiceNow.

Creating a Helpdesk Policy

1. Using the Policy Wizard, create a controlling policy that elevates requiring approval.
2. Select what file types you want targeted with the approval elevation.
3. Choose your targets. You can specify several different targets.
4. Name your policy and click **Create**.



The important wizard added actions on this policy are:

- **Approval Request From Action**
- **Restrict File Dialogs**
- **Add Administrative Rights**.

5. Set the **Inactive** switch to **Active**.

Once the agent receives the update, users receive a message action dialog to enter their written request in the Reason (required) field which then sends a request to either the Privilege Manager console or integrated Helpdesk.

Workflow

When end users try to open a restricted application, they must enter a reason for needing the application and send it for approval. While the request is being evaluated, whenever end users start the application a status pending message will appear. Once the request has been approved or denied, end users receive an approval or denial.

Approve requests

To approve or deny requests in the Privilege Manager Console, go to **Admin: Tools | Manage Approvals** to view all application requests.

Offline Approvals

Approval workflows usually require a workstation to be online to send out the approval request and then receive an approval for an application to continue to run or execute. If a workstation is offline, an end user needs a way to also request an approval for an application to continue to execute, for such a situation an Offline Approval process has been implemented.

During an offline approval process a prompt is triggered for a 6-digit numeric pin also called request code. The end user then calls the help desk and provides system information to the help desk representative. The help desk representative generates and provides a 12-character alphanumeric response code for the deployed policy residing on the offline workstation. Once the end user enters the response code the application execution continues and other actions can be performed, for example adding administrative rights.

The message actions used in the Offline Approval policy are OS specific. Use the action:

Windows:

macOS:

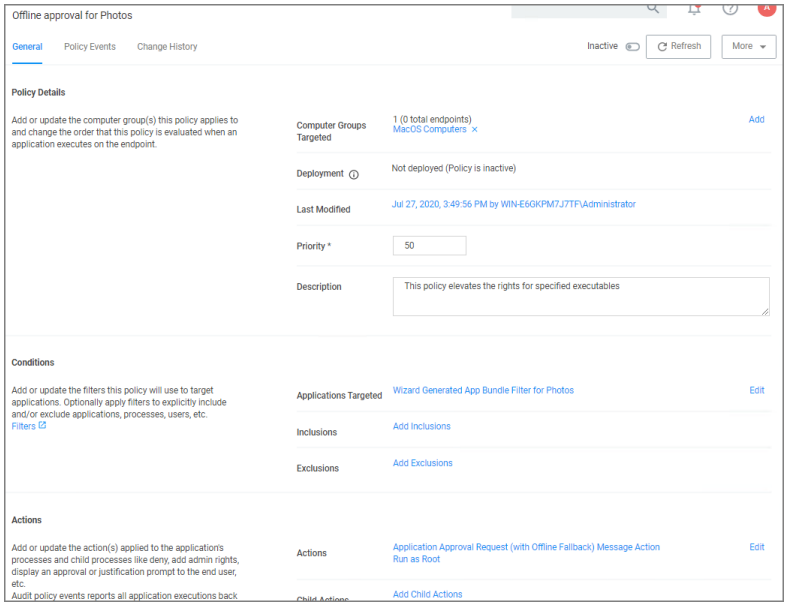
Notifications for approvals can also be issued to mobile devices. Refer to Mobile App section - Configure the Notification Settings

Creating an Offline Approval Policy

For offline approvals to work, a message action supporting offline fallback needs to be configured. This example uses the macOS based message action.

1. Create an Offline Approval Policy, by specifying the specific message action:
   a. Navigate to Actions and click **Edit**.
   b. Search for and **Add** the action **Application Approval Request (with Offline Fallback) Message Action**.
   c. Click **Update**.

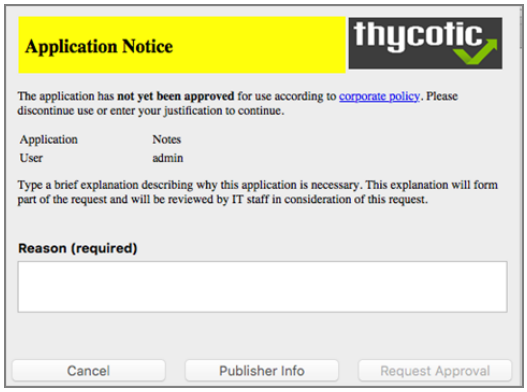
2. Click **Save Changes**.



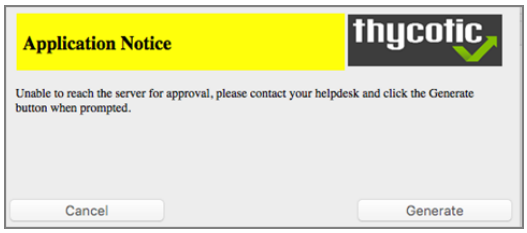
Workstation Offline Approval

When the policy created above applies, the system first attempts an online approval request and if the server is unavailable it uses the request and response codes to verify authorization.

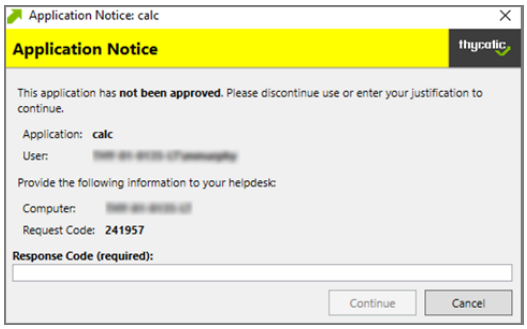
1. When trying to install an application that is not explicitly white-listed via policy while offline, the following Application Notice opens:



2. When the system is offline, the following notice opens:



3. Follow the instructions to contact your help desk and only click **Generate** when prompted.
4. You will then see:



   Provide the information to the help desk, they will need the 6-digit code, in this example 191279, to create a response code.

5. Once your help desk contact verifies the authenticity of the request, you will be provided a 12-digit **Response Code** that needs to be entered in the text field.
6. Click **Continue** after entering the Response Code.

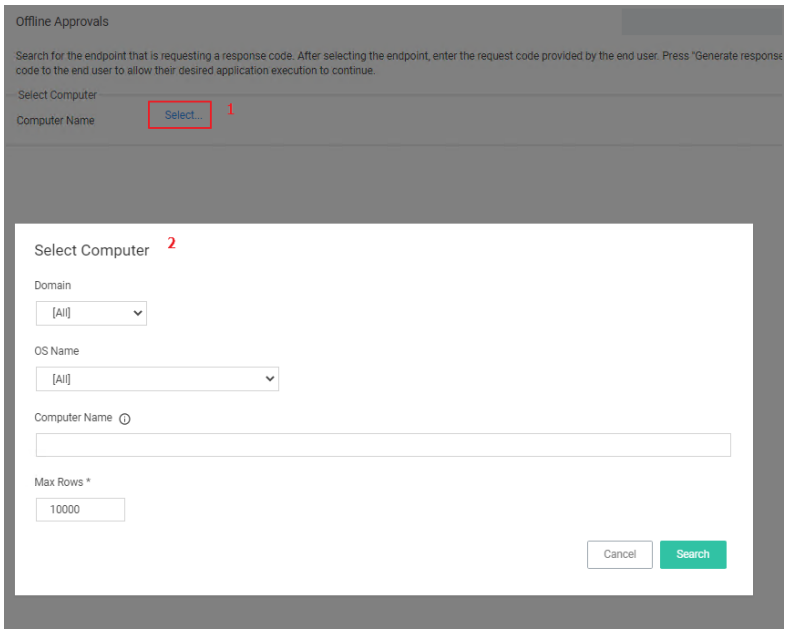
At this point the application installation should be able to continue.

Privilege Manager Offline Approval

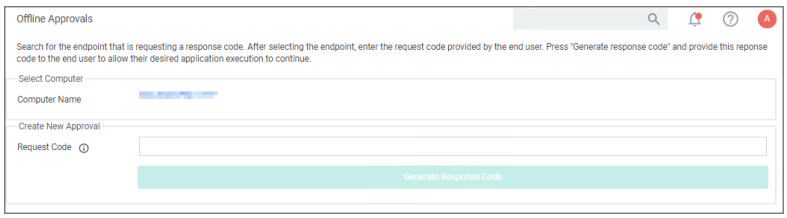
The following procedures provides detailed steps about the offline approval process in the Privilege Manager UI.

1. Navigate to **Admin | Tools | Offline Approval**.
2. Click **Select...** and search to access the list of Computers with open offline approval requests.

Computer Groups



3. Verify the customer's name is in the list.
4. Select the customer's computer from the list and click the **Select** button.



5. Enter the **Request Code** provided by the customer and click **Generate Response Code**.
6. Read the Response Code back to the customer to enter at the endpoint.

XML for Challenge Response Message Action


```
<?xml version="1.0" encoding="ISO-8859-1"?>

<CustomXamlExecutionActionContract xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schema
instance" xmlns="http://schemas.arellia.com/dc/ApplicationControl/ApplicationAction/">
    <adc:Description>This action will display a customized message to the user, allowing for a challe
    <adc:FolderId>26bc9625-ed2b-4e45-9377-a3efb4462118</adc:FolderId>
    <adc:ItemId>9ea45416-f3f5-4dac-abcd-6d8ef94c9316</adc:ItemId>
    <adc:Name>Challenge/Response Message Action</adc:Name>
    <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
    <adc:Strings />
    <adc:Tags />
    <AdjustSession>false</AdjustSession>
    <Commandline i:nil="true" />
    <Executable>.\ArelliaDisplayXamlAction.exe</Executable>
```

```
    <TerminateExitCode>100</TerminateExitCode>
    <WaitOnApplication>true</WaitOnApplication>
    <ChildAssociations />
    <OfflineApprovalType>OfflineNotAllowed</OfflineApprovalType>
    <OwnsItemIds />
    <RequireLogon>false</RequireLogon>
    <UserGroupId i:nil="true" />
    <Xaml><![CDATA[
<Window
    xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
    xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"
    xmlns:sys="clr-namespace:System;assembly=mscorlib"
    xmlns:adx="http://schemas.arellia.com/winfx/2012/arelliadisplayxamlaction"
    xmlns:ac="http://schemas.arellia.com/winfx/2010/xaml"
    xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006"
    mc:Ignorable="ac"
    Icon="Images/thycotic-icon.png"
    WindowStartupLocation="CenterScreen"
    Title="{DynamicResource WindowTitle}"
    ResizeMode="NoResize"
    SizeToContent="WidthAndHeight">

    <Window.Resources>



        <Style x:Key="BaseLabelStyle" TargetType="TextBlock">
            <Setter Property="Margin" Value="10,3" />
        </Style>

        <Style x:Key="BaseButtonStyle" TargetType="Button">
            <Setter Property="Padding" Value="15,3" />
            <Setter Property="MinHeight" Value="25" />
            <Setter Property="MinWidth" Value="85" />
            <Setter Property="Margin" Value="8,0,0,0" />
        </Style>

        <Style x:Key="ReadOnlyFieldStyle" TargetType="TextBlock">
            <Setter Property="FontWeight" Value="Bold" />
            <Setter Property="VerticalAlignment" Value="Center" />
            <Setter Property="TextWrapping" Value="Wrap" />
        </Style>

        <Style x:Key="BaseRichTextBoxStyle" TargetType="RichTextBox">
            <Setter Property="BorderThickness" Value="0" />
            <Setter Property="Background" Value="Transparent" />
            <Setter Property="Padding" Value="0" />
            <Setter Property="IsReadOnly" Value="True" />
            <Setter Property="IsTabStop" Value="False" />
        </Style>
```

```
        <sys:String
x:Key="EncodedLogoImage">iVBORw0KGgoAAAANSUhEUgAAAQcAAABYCAIAAAB3ZqVmAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
E+KKFgRbnwEinf8kMjc3B92Nj7iiQ8HWZ4CoU0nrCtd1scFMfPnll9CZsHVF5Mqg+tiMq+wZLkHGUd8b/vZw2iZdssyw5pFFsPUZI
uoKAqlDIMBQlCvUcSvNZCYN27dvV2nDhLd8AuF14NaH6imhWuewK6zWP1gpH3zmga4GNeTjjz9GLDdIOi+wrqBNSb25zvT0NNaOAb
27UMsAUQyETbTrWHHx4kXUMkCnI664BnQxEDYBRQgEGApxRTOO5e3qClTxQKdDruBmmzKDAgibgCIEAgwyVkRAjAEiHcR4lCzNeTO
SQYwHugBU8UDXkogr7NqFWgaIcoBEDBDFQJgBIh3EGCDSQYwHugBU8UDXkogr7NqFWgaIcpDwzDkBUQyEGSDSQYwBIh3EeKALQBUP
ICgbAXWQ/KOPPkLMxNDQEKQ6CDNApIMYD3Q1UMsAkQ5iDBDFcMslOu2mNxNv0ml0tPdzRS1rpINcgXeWIHsIBEzQt3z++efhXmvlu
u/Zs+fcuXNYLAQ55+DBg5VKJay3hZattyghT56vUFCGDEkaLlLf7PS6evXqY8eOXb16lTZO3Sfqzbvvvrtlyx YlJupvTJQct5zZEl
lxRcDevXvrTqhflUKMoa7vHIKjqveLlT+p9/gOhSY29Dp1ulsdlYuF+nGGW9e7TvXQicTS6A7O/JGw5E7MdoYrCPTlgnjvvfeQt/N
zlbRl8tRXqtWlyMLjlPtd/z8JSlajROC94Fd4p4vsyeIKIRX+n2i4pfGZnomT3RMn6dWuVJYtQSIGmjg5jkud2+r/zsgSk8EoUext
Hh7vF1cI+XArnutsfuXWLQdvo9dO5fbarcBov08udIZdHSj+9xtxxBVCAdCI8ccDd9TK7VzZ9LfbHn359izn1sE97BUP/Bjf12TEF
K5CYII=</sys:String>


        <sys:String x:Key="WindowTitle">Justify Application Usage</sys:String>



        <Style x:Key="MainWindowPanelStyle" TargetType="Panel">
            <Setter Property="Width" Value="500" />
            <Setter Property="Background" Value="#FFF0F0F0" />
        </Style>

        <Style x:Key="HeadingBorderStyle" TargetType="Border">
            <Setter Property="BorderThickness" Value="0,0,0,1" />
            <Setter Property="BorderBrush" Value="#FF777777" />
        </Style>

        <Style x:Key="TitleHeadingBorderStyle" TargetType="Border">
            <Setter Property="Grid.Column" Value="0" />
            <Setter Property="Padding" Value="8" />
            <Setter Property="Background" Value="Yellow" />
        </Style>

        <Style x:Key="TitleHeadingStyle" TargetType="TextBlock">
            <Setter Property="Text" Value="Application Notice" />
            <Setter Property="FontSize" Value="16" />
            <Setter Property="FontWeight" Value="Bold" />
            <Setter Property="Foreground" Value="Black" />
        </Style>

        <Style x:Key="ImageHeadingBorderStyle" TargetType="Border">
            <Setter Property="Grid.Column" Value="1" />
            <Setter Property="Padding" Value="8" />
            <Setter Property="Background" Value="#3d3d3d" />
        </Style>

        <Style x:Key="ImageHeadingStyle" TargetType="Image">
            <Setter Property="Grid.Column" Value="1" />
            <Setter Property="Height" Value="18" />
            <!-- <Setter Property="FlowDirection" Value="{Binding [FlowDirection],Source={StaticResou
        </Style>
        <!--
```

```
        <Style x:Key="ImageHeadingBorderStyle" TargetType="Border">
            <Setter Property="Grid.Column" Value="1" />
            <Setter Property="Padding" Value="8" />
            <Setter Property="Background" Value="Black" />
        </Style>

        <Style x:Key="ImageHeadingStyle" TargetType="Image">
            <Setter Property="Grid.Column" Value="1" />
            <Setter Property="Source" Value="Images/logo-white.png" />
            <Setter Property="Height" Value="18" />
        </Style>
-->


        <Style x:Key="ContentPanelStyle" TargetType="Panel">
            <Setter Property="Margin" Value="8" />
        </Style>

        <Style x:Key="InformationRichTextBoxStyle" TargetType="RichTextBox" BasedOn="{StaticResource
            <Setter Property="Margin" Value="0,8,0,0" />
        </Style>

        <Section x:Key="InformationTextSection" xml:space="preserve">
            <Paragraph FontFamily="Segoe UI" FontSize="12"><Run>This application has </Run><Bold>not
        </Section>

        <Style x:Key="PropertiesPanelStyle" TargetType="Panel">
            <Setter Property="Margin" Value="0,8,0,0" />
        </Style>

        <Style x:Key="ApplicationNameLabelStyle" TargetType="TextBlock" BasedOn="{StaticResource Base
            <Setter Property="Grid.Row" Value="0" />
            <Setter Property="Text" Value="Application:" />
        </Style>

        <Style x:Key="ApplicationFieldStyle" TargetType="TextBlock" BasedOn="{StaticResource ReadOnly
            <Setter Property="Grid.Row" Value="0" />
            <Setter Property="Grid.Column" Value="1" />
            <Setter Property="Text" Value="{Binding ProcessName}" />
        </Style>

        <Style x:Key="UserNameLabelStyle" TargetType="TextBlock" BasedOn="{StaticResource BaseLabelSty
            <Setter Property="Grid.Row" Value="1" />
            <Setter Property="Text" Value="User:" />
        </Style>

        <Style x:Key="UserNameFieldStyle" TargetType="TextBlock" BasedOn="{StaticResource ReadOnlyFie
            <Setter Property="Grid.Row" Value="1" />
            <Setter Property="Grid.Column" Value="1" />
            <Setter Property="Text" Value="{Binding UserName}" />
        </Style>

        <Style x:Key="InstructionRichTextBoxStyle" TargetType="RichTextBox" BasedOn="{StaticResource
```

```
        <Setter Property="Margin" Value="0,8,0,0" />
    </Style>

    <Section x:Key="InstructionTextSection" xml:space="preserve">
        <Paragraph FontFamily="Segoe UI" FontSize="12"><Run>Please enter your Google Authenticato
    </Section>

    <Style x:Key="ChallengeResponsePanelStyle" TargetType="Panel">
        <Setter Property="Margin" Value="0,8,0,5" />
    </Style>

    <Style x:Key="ChallengeLabelStyle" TargetType="TextBlock" BasedOn="{StaticResource BaseLabelS
        <Setter Property="Text" Value="Request code:" />
        <Setter Property="Grid.Row" Value="0" />
        <Setter Property="Grid.Column" Value="0" />
    </Style>

    <Style x:Key="ChallengeTextStyle" TargetType="TextBlock">
        <Setter Property="Text" Value="{Binding ChallengeToken,Mode=OneWay}" />
        <Setter Property="VerticalAlignment" Value="Center" />
        <Setter Property="FontWeight" Value="Bold" />
        <Setter Property="FontSize" Value="15" />
        <Setter Property="Margin" Value="0,0,0,8" />
        <Setter Property="Grid.Row" Value="0" />
        <Setter Property="Grid.Column" Value="1" />
    </Style>

    <Style x:Key="ResponseLabelStyle" TargetType="TextBlock" BasedOn="{StaticResource BaseLabelSty
        <Setter Property="Text" Value="Validation code:" />
        <Setter Property="Grid.Row" Value="1" />
        <Setter Property="Grid.Column" Value="0" />
    </Style>

    <Style x:Key="ResponseTextBoxStyle" TargetType="TextBox">
        <Setter Property="Grid.Row" Value="1" />
        <Setter Property="Grid.Column" Value="1" />
        <Setter Property="MaxLength" Value="40" />
        <Setter Property="Text" Value="{Binding ResponseToken,Mode=TwoWay,UpdateSourceTrigger=Prop
    </Style>

    <Style x:Key="ButtonPanelStyle" TargetType="StackPanel">
        <Setter Property="Orientation" Value="Horizontal" />
        <Setter Property="HorizontalAlignment" Value="Right" />
        <Setter Property="Margin" Value="0,8,0,0" />
    </Style>

    <Style x:Key="ContinueButtonStyle" TargetType="Button" BasedOn="{StaticResource BaseButtonSty
        <Setter Property="Content" Value="Continue" />
        <Setter Property="Command" Value="{Binding ContinueWithChallengeResponseCommand}" />
        <Setter Property="CommandParameter" Value="{Binding ResponseToken}" />
    </Style>

    <Style x:Key="CloseButtonStyle" TargetType="Button" BasedOn="{StaticResource BaseButtonStyle}
```

```
            <Setter Property="Content" Value="Cancel" />
            <Setter Property="Command" Value="{Binding CloseCommand}" />
        </Style>

    </Window.Resources>

    <StackPanel Style="{StaticResource MainWindowPanelStyle}"
                    adx:WindowHelper.Title="{Binding Result,Source={StaticResource WindowTitle}}">

        <Border Style="{StaticResource HeadingBorderStyle}">
            <Grid>
                <Grid.ColumnDefinitions>
                    <ColumnDefinition Width="*" />
                    <ColumnDefinition Width="Auto" />
                </Grid.ColumnDefinitions>

                <Border Style="{StaticResource TitleHeadingBorderStyle}">
                    <TextBlock Style="{StaticResource TitleHeadingStyle}" />
                </Border>
                <Border Style="{StaticResource ImageHeadingBorderStyle}">

                    <Image Style="{StaticResource ImageHeadingStyle}"
                             adx:ImageSourceHelper.EncodedImage="{StaticResource EncodedLogoImage}" />
                </Border>
            </Grid>
        </Border>

        <StackPanel Style="{StaticResource ContentPanelStyle}">


            <RichTextBox Style="{StaticResource InformationRichTextBoxStyle}"
                         ac:RichTextBoxHelper.Section="{StaticResource InformationTextSection}"
                         adx:RichTextBoxHelper.Section="{StaticResource InformationTextSection}" />


            <Grid Style="{StaticResource PropertiesPanelStyle}">
                <Grid.ColumnDefinitions>
                    <ColumnDefinition Width="Auto" />
                    <ColumnDefinition Width="*" />
                </Grid.ColumnDefinitions>
                <Grid.RowDefinitions>
                    <RowDefinition />
                    <RowDefinition />
                </Grid.RowDefinitions>

                <TextBlock Style="{StaticResource ApplicationNameLabelStyle}" />
                <TextBlock Style="{StaticResource ApplicationFieldStyle}" />

                <TextBlock Style="{StaticResource UserNameLabelStyle}" />
                <TextBlock Style="{StaticResource UserNameFieldStyle}" />

            </Grid>
```

```
            <RichTextBox Style="{StaticResource InstructionRichTextBoxStyle}"
                         ac:RichTextBoxHelper.Section="{StaticResource InstructionTextSection}"
                         adx:RichTextBoxHelper.Section="{StaticResource InstructionTextSection}" />

            <Grid Style="{StaticResource ChallengeResponsePanelStyle}">
                <Grid.ColumnDefinitions>
                    <ColumnDefinition Width="Auto" />
                    <ColumnDefinition Width="*" />
                </Grid.ColumnDefinitions>
                <Grid.RowDefinitions>
                    <RowDefinition />
                    <RowDefinition />
                </Grid.RowDefinitions>


                <!-- <TextBlock Style="{StaticResource ChallengeLabelStyle}" />
                <TextBlock Style="{StaticResource ChallengeTextStyle}" />
                -->


                <TextBlock Style="{StaticResource ResponseLabelStyle}" />
                <TextBox Style="{StaticResource ResponseTextBoxStyle}" />
            </Grid>


            <StackPanel Style="{StaticResource ButtonPanelStyle}">
                <Button Style="{StaticResource ContinueButtonStyle}"
                          adx:ButtonHelper.IsDefault="true" />
                <Button Style="{StaticResource CloseButtonStyle}"
                          adx:ButtonHelper.IsCancel="true" />
            </StackPanel>

        </StackPanel>
    </StackPanel>
</Window>
             ]]></Xaml>
</CustomXamlExecutionActionContract>
```

Blocking Policies

Blocking is a policy that denies applications from running on your endpoints based on application attributes, file hash, location, or certificates. This is a powerful type of policy and it may be used to block specific, known and unwanted applications from running. A block policy can target programs that prevent productivity for your end users or applications that are known malware. If malware, you can also add a quarantine action for your block policy as outlined in the second example below.

Delinea Privilege Manager controls any application on a machine. When you configure Privilege Manager correctly, targeted applications can be elevated, allow listed, or blocked. But if you create new policies without careful consideration then you can potentially block core system processes.

Before you create new polices, keep in mind the following best practices:

- Do not enable policies until after you have configured them. As a safety precaution, all newly-created application control policies are turned off until you enable them.
- Important: New policies that you create will automatically target all applications until you add application filters that will narrow the scope.
- Additionally, Delinea highly recommends testing all policies on a limited number of machines before they are deployed to the entire environment. See Best practices for Application Control Solution policies for more information.

The following examples are available:

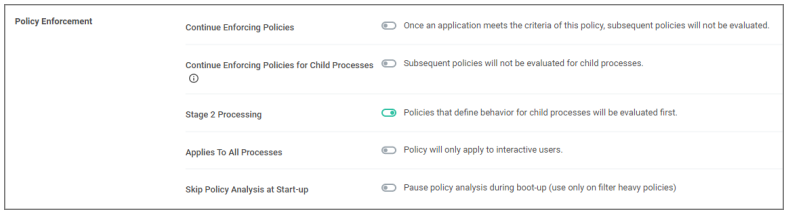
- Blocking Specific Applications
- iTunes with File Upload
- Quarantine Specific Malware
- Catch-all block Policy

Catch-all Deny

A catch-all deny policy is the last policy executed following the execution of a group of allow list policies. This enables you to configure your allow list to allow approved applications, like the Windows directory or other installed applications, and then to deny everything else, like applications downloaded from the internet or a thumb drive.

To create a catch-all deny policy, follow these steps:

1. Under your Computer Group select Application Policies and click **Create Policy**.
2. Select **Skip the wizard, take me to a blank policy** to create a blank policy.
3. Enter a name and description, change the default priority value to a higher number, for example 99 and click **Create**.
4. Under **Conditions**, click **Add Exclusions**.
5. Search for and **Add** the **LocalSystem and Service applications** filter.
6. Click **Update**.
7. On the bottom of the policy page, click **Show Advanced**.
8. Under **Policy Enforcement**, ensure only **Stage 2 processing** is set to active.



9. Click **Save Changes**.
10. Set the **Inactive** switch to **Active**.

If you are creating a new catch-all policy to be used in conjunction with allow list policies, please verify that the allow list is catching all system applications and that the new deny policy is the last policy executed. For additional safety you can define the exclude any parameter to exclude system and service applications.

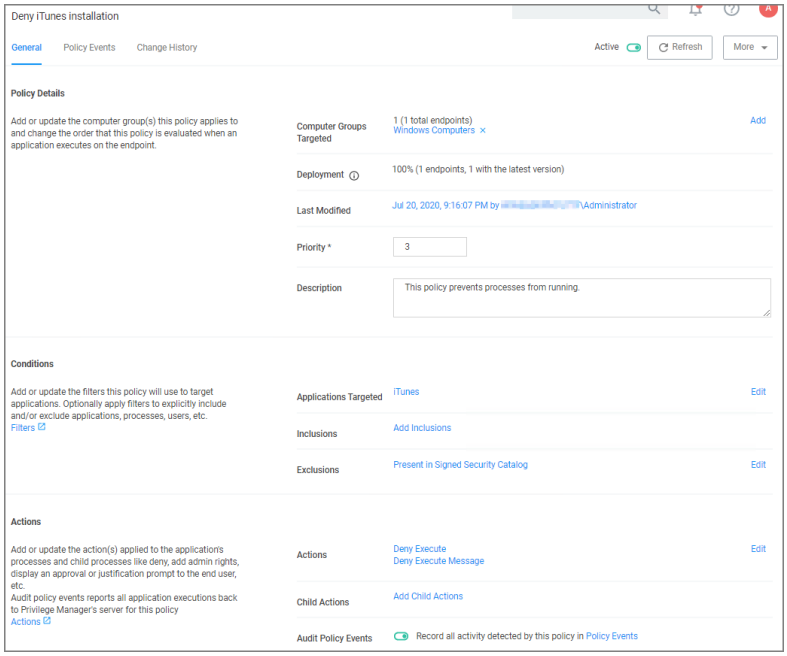
iTunes with File Upload

As we've seen, there are multiple ways to introduce a new application into Privilege Manager before assigning a policy to it. For this example we will perform a File Upload for the iTunes installer to quickly deny list the iTunes program from running on target endpoints.

> **Note:** When the iTunes default filter is used, verify the correct Company name is entered to match the application targeted by the policy.

1. Using the Policy Wizard, create a controlling policy that blocks application execution on endpoints.
2. Select how you want the processes blocked, either **Block Silently** or **Notify and Block**, for this example we use **Block Silently**. Click **Next Step**.
3. Select what types you want the policy to block, for this example it's **Executables**.
4. Choose your target, for this example **File Upload**.
5. Click **Choose File** and select the installer (iTunes.exe) to upload.
6. Click **Upload File**.
7. On the **Manage Application** page select all the identifying factors you want the filter to target.
8. Click **Create Filter**.
9. Click **Next Step**.
10. Name your policy and add a description, click **Create Policy**.

11. Set the **Inactive** switch to **Active**.



Under the Actions tab, do not change the settings, but notice it is set to Deny Execute Message. This will produce a pop-up message to the user telling them this application execution is denied.

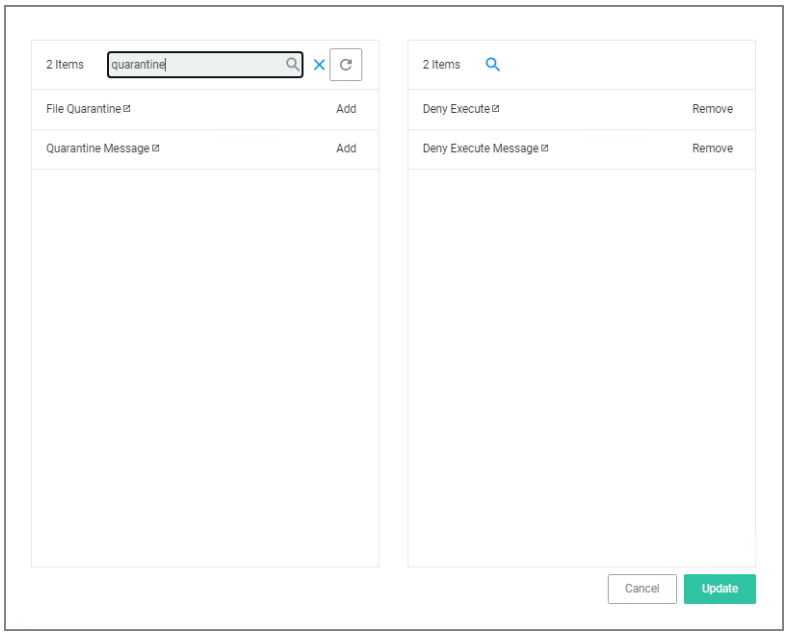
You can edit the policy further, if needed. Adjust the Policy Priority as needed.

Quarantine Specified Malware

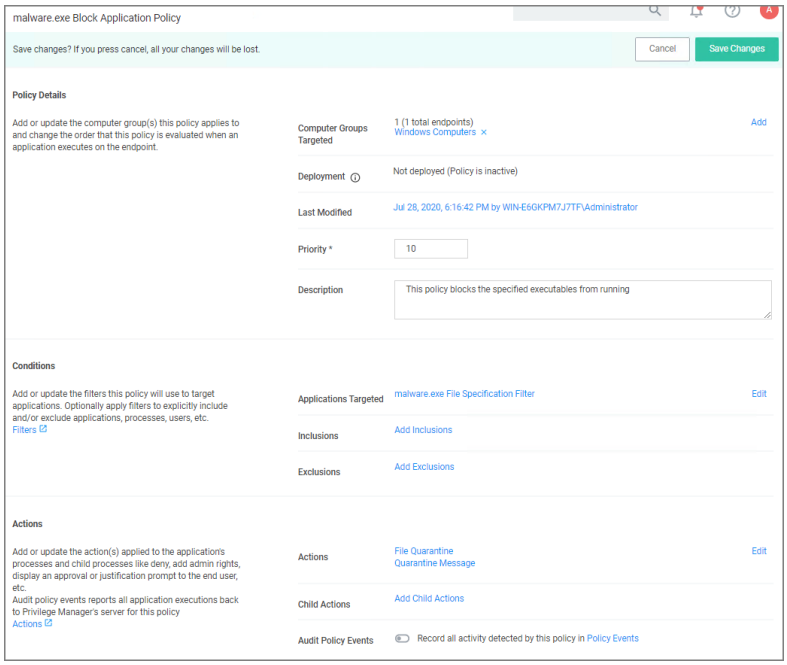
For known cases of malware or ransomware, you can use Privilege Manager to prevent specified applications from running and place them in a quarantine. For this example we'll target the generic executable “malware.exe,” but you can do this with any file name.

1. Navigate to **Admin | Filters** and click **Create Filter**.
2. From the platform drop-down select the OS to target, for this example **Windows**.
3. From the type drop-down select **File Specification Filter**.
4. Add a Name and Description, click **Create**.
5. On the filter page, under **Settings: File Names** type **malware.exe**.
6. Click **Save Changes**.
7. Under you Computer Group, select **Application Policies**.
8. Using the Policy Wizard, create a controlling policy that blocks application execution on endpoints.
9. Select how you want the processes blocked, either **Block Silently** or **Notify and Block**, for this example we use **Block Silently**. Click **Next Step**.
10. Select what types you want the policy to block, for this example it's **Executables**.
11. Choose your target, for this example **Existing Filter**.

12. Search for and **Add** the **malware.exe** filter created in the above steps.
13. Click **Update**.
14. Click **Next Step**.
15. Name your policy and add a description, click **Create Policy**.
16. Under **Actions**, click **Edit**.
17. Search for **quarantine** and **Add** the **File Quarantine** and **Quarantine Message** actions.
18. **Remove** the **Deny Execute** and **Deny Execute Message** actions.



19. Click **Update**.



20. Click **Save Changes**.
21. Set the **Inactive** switch to **Active**.

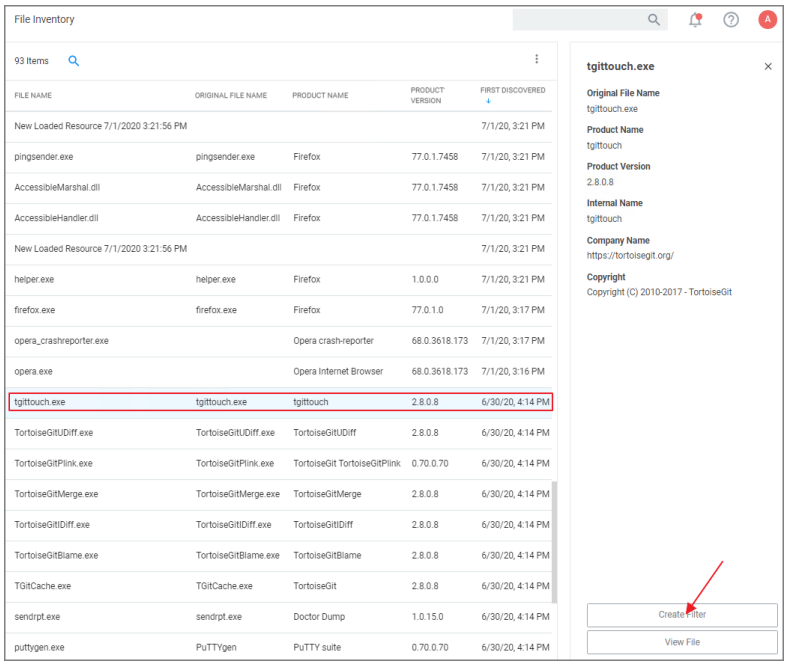
Once this policy has been applied to your endpoint/s, any executable called malware.exe will be automatically blocked and quarantined if prompted to run

Specific Applications

Using File Inventory

To create a new policy using file inventory data to block specific applications, follow these steps:

1. From the navigation menu select **File Inventory**.
2. From the table grid of inventoried files, select the application you want to block.



3. Click **Create Filter**.
4. On the **Manage Application** page select all the identifying factors you want the filter to target.
5. Click **Create Filter** or **Create and Add to Policy**. Use the **Create and Add to Policy** option if you already have a deny policy to target applications.

   Otherwise use **Create Filter** and then use the Policy Wizard or a blank policy to add that filter.

Using the Policy Wizard

To create a new policy using the policy wizard to block specific applications, follow these steps:

1. Using the Policy Wizard, create a controlling policy that blocks application execution on endpoints.
2. Select how you want the processes blocked, either **Block Silently** or **Notify and Block**, for this example we use **Block Silently**. Click **Next Step**.
3. Select what types you want the policy to block, for this example it's **Executables**.
4. Choose your target, for this example **File Upload**.
5. Click **Choose File** and select a file to upload.
6. Click **Upload File**.
7. On the **Manage Application** page select all the identifying factors you want the filter to target.
8. Click **Create Filter**.
9. Click **Next Step**.
10. Name your policy and add a description, click **Create Policy**.
11. Set the **Inactive** switch to **Active**.

Be sure to test the new policy on a few machines before you roll it out to the environment.

Elevation Policies

Distinct from allow policies where applications are simply allowed to run with default user level privileges, an Elevation Policy will apply Administrator credentials to specified applications. This type of policy is often paired with allowlisting to save IT Administrators time when many employees must perform trusted tasks that require Administrator credentials to complete, like installing a trusted application (Adobe) or device (printer).

In Privilege Manager v10.7 the Restrict File Dialogs action has been added to the product. Delinea recommends using this action on elevation policies to prevent the misuse of file open and save dialogs for elevated applications.

Topics in this section:

- Setting up ActiveX Policies
- UAC Override Policy
- Elevate Applications launched from Network Share Policy
- Elevate msi launched from a Network Share
- Elevate Applications whose Execution Requires Approval
- Elevate Applications that Require User Justification
- MS Visual Studio Installations - Filters and policy now provided via Configuration Feeds. Refer to Config Feeds for download and installation information.

Setting up ActiveX Policies

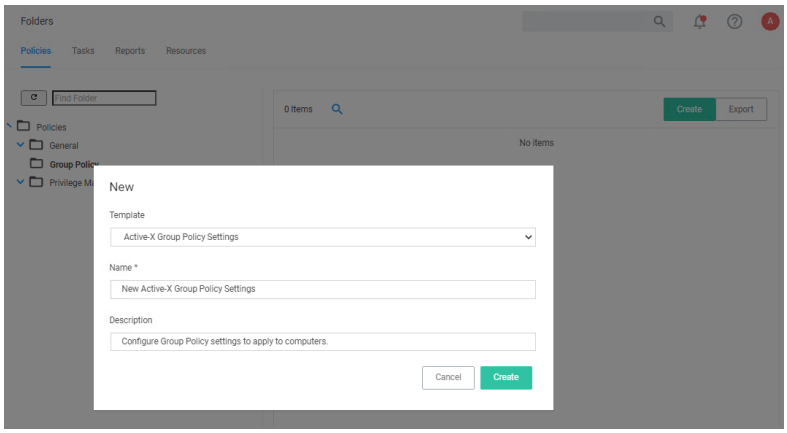
To allow add-ins to be installed via Internet Explorer, you need to create an allow policy for ActiveX.

Note: You will need to import local group policy definitions before editing your Active-X Group Policy Settings.

Refer to the Local Security topic, specifically Manage Local Groups.

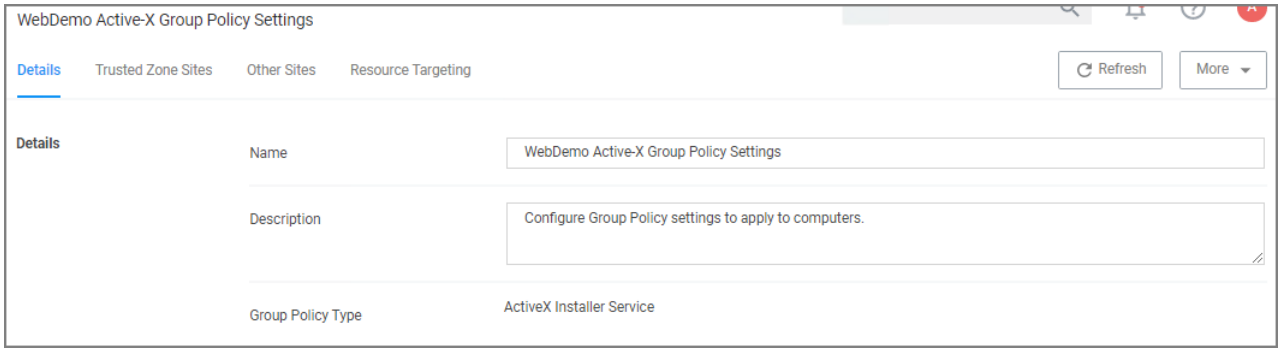
Creating the Policy

1. Navigate to **Admin | Folders**.
2. Select **Group Policies**.
3. Click **Create**.



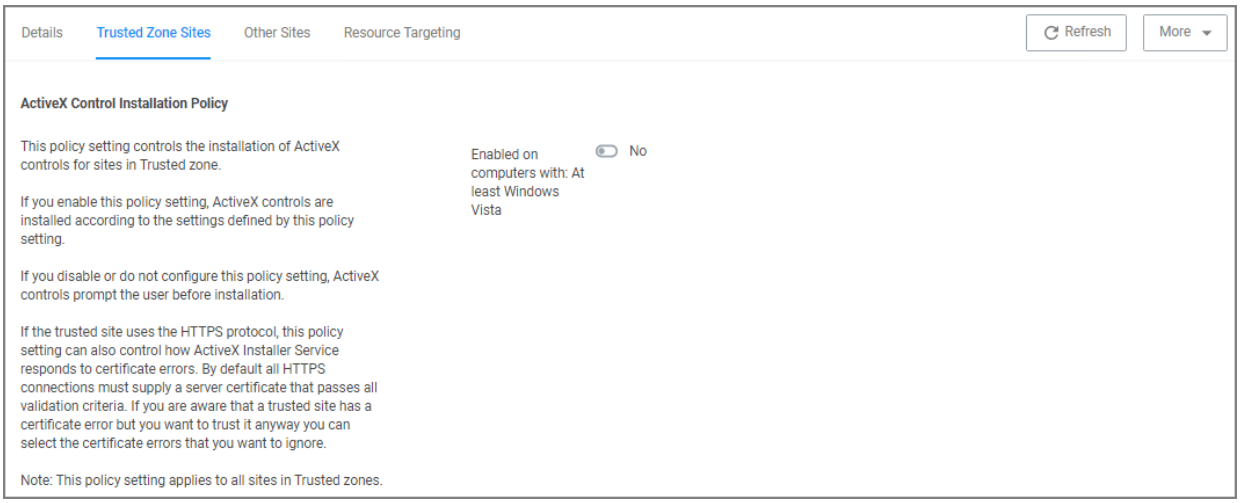
4. From the **Template** drop-down, select **Active-X Group Policy Settings**.
5. Enter a name and description to identify the policy.
6. Click **Create**.
7. If you haven't already imported the Local Group Policy Definitions, Privilege Manager prompts you to import the definitions.

Click **Go to Import Task** and run the task. Return to the Active-X policy.

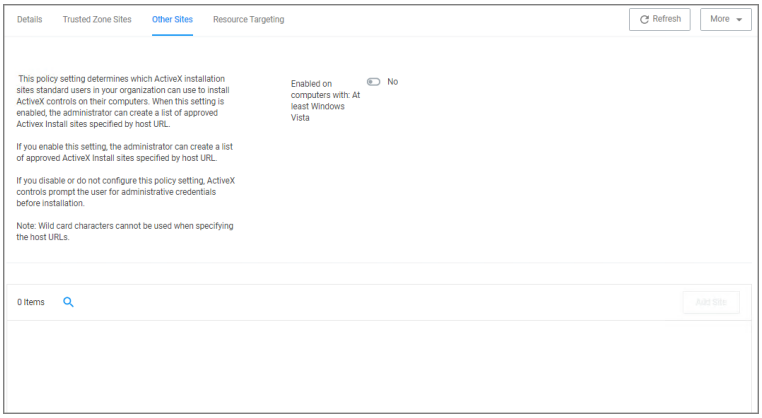


8. You can now add Trusted Zone sites and Other Sites and customize what actions to take when they are accessed.

- Trusted Zone Sites tab:

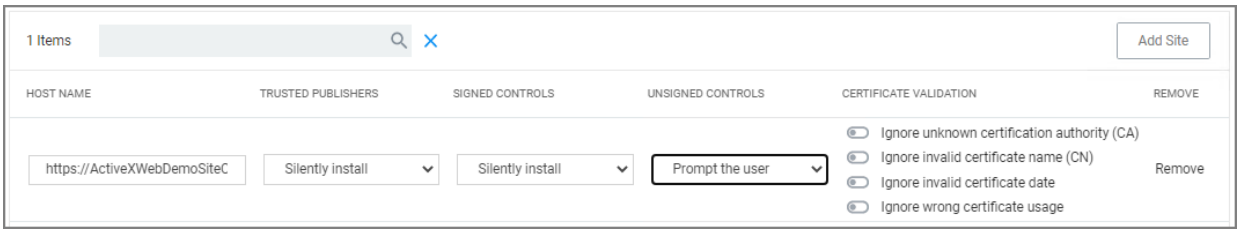


- Other Sites tab:



a. To customize, set the **Enabled on computers with: At least Windows Vista** to **Yes**.

b. Click **Add Site**.



c. Enter the Host Name (URL) for the site.

d. Select from the Trusted Publishers and Signed Controls drop-down. The options are

- Don't install
- Prompt the user
- Silently install

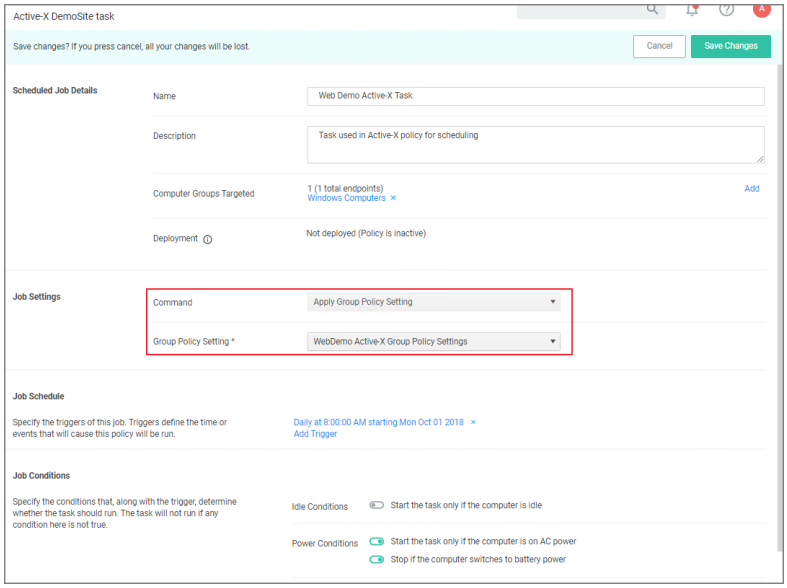
e. Select from the Unsigned Controls drop-down. The options are

- Don't install
- Prompt the user

f. Set any of the Certificate Validations switches to active specific ignore behavior, such as

- Ignore unknown certification authority (CA)
- Ignore invalid certificate name (CN)
- Ignore invalid certificate date
- Ignore wrong certificate usage

9. Click **Save Changes**.
10. On the **Resource Targeting** tab, Privilege Manager provides instructions for setting up how to deploy the Active-X policy to Resource Targets.
11. In **Clone the following Policy**, click the **Policy** link to open the read-only client task.
12. Duplicate the client task and give it a name identifying it as the task for your Active-X policy.



a. From the **Job Settings | Command** drop-down, select **Apply Group Policy Settings**.

b. From the **Group Policy Setting** drop-down, select the Active-X policy created above.

> **Note:** Apply Group Policy Settings when you have 2 or more ActiveX policies to add to the Parameters, otherwise use the Apply Group Policy Setting item.

13. Under Job Schedule modify the schedule and/or add triggers.
14. Set the **Inactive** switch to **Active**.
15. Click **Save Changes**.

On completing this configuration, Privilege Manager Triggers feature will then send the configured task to the targeted endpoint.

To view the Task, go to the **Task Scheduler**. You must have administrator access to view the task inside Thycotic folder.

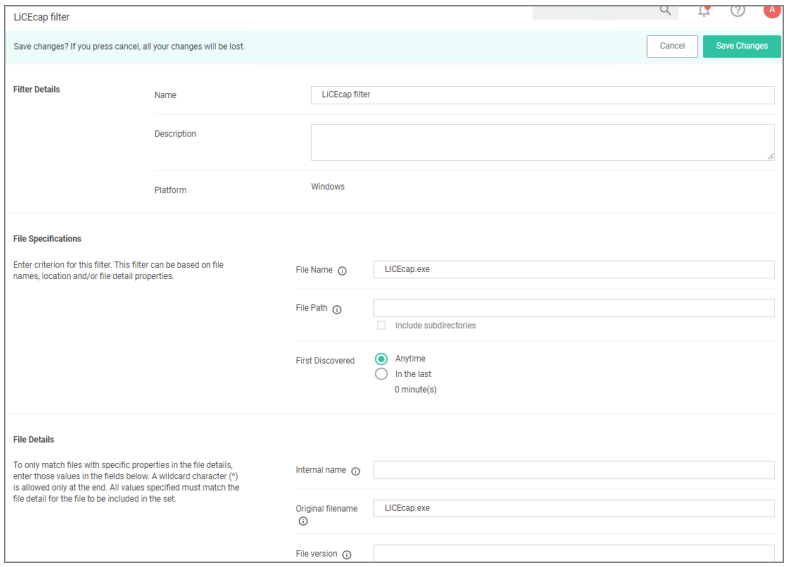
Application Execution Requires Approval

This policy type requires a user to provide a justification reason as to why they need to run a process (installer or executable). Then, the reason is submitted to specified managers via Privilege Manager**Admin: Tools | Manage Approvals** for approval. It also depends on whether or not the Manual Approval process is used. For instance, if you have configured Service Now as your approval process handler, these approval requests won't appear in the **Admin: Tools | Manage Approvals** area. There are several pieces to the Actions in this policy. Because Conditions and Actions are independent, these actions for approval can be applied to any condition. In this use case, we will apply this action to the LICEcap gif creator.
First create a filter that will identify the process/executable on which Privilege Manager will act.

1. Navigate to **Admin | Filters**.
2. Click **Create Filter**.

   Note: In this use case, we will target the LICEcap application (LICEcap.exe).

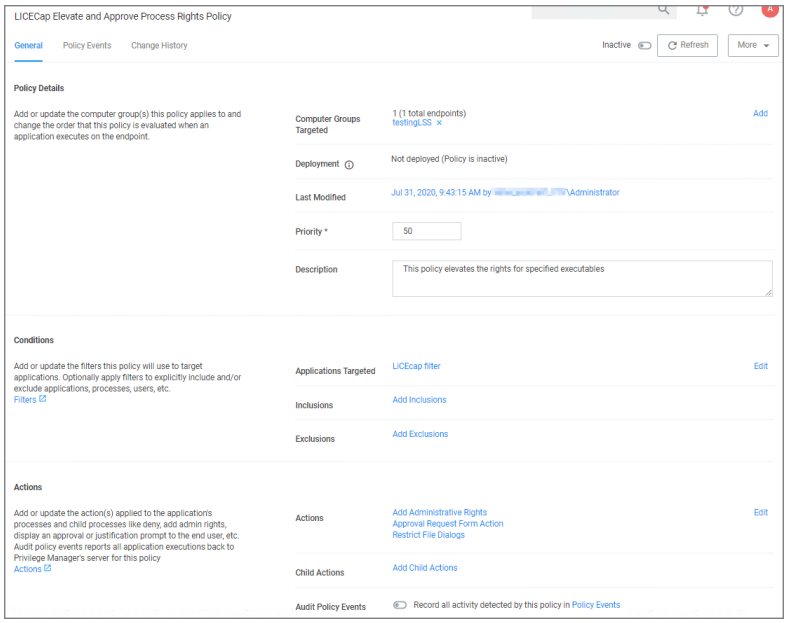
3. From the **Platform** drop-down select **Windows**.
4. From the **Filter Type** drop-down select **Blank Win32 Executable Filter**.
5. Add a name and description, click **Create**.
6. Enter **LICEcap.exe** in the File Name field under File Specifications as well as in the Original filename field under File Details.



7. Click **Save Changes**.

Create a Policy using this Filter

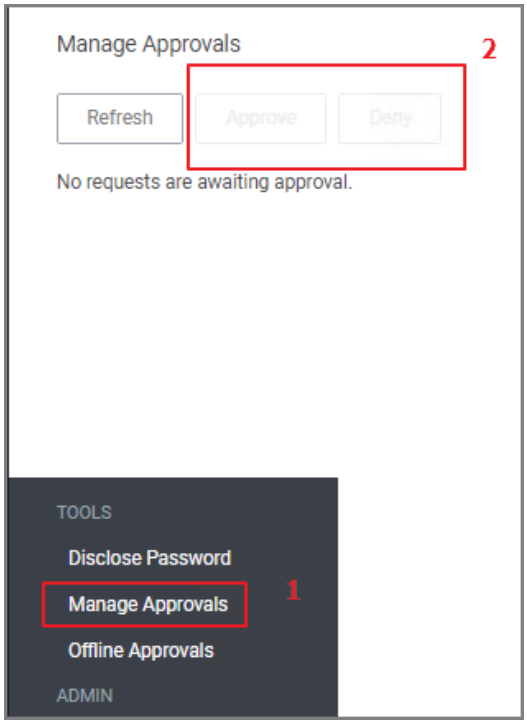
1. Using the Policy Wizard, create a controlling policy that elevates requiring approval.
2. Select what file types you want targeted with the approval elevation, for this example select **Executables**.
3. Choose your targets. You can specify several different targets, for this example select **Existing Filter**.
4. Search for and add the LICEcap filter created previously.
5. Click **Update**. You may also use **File Upload** to upload the LICEcap.exe file or **Inventoried File** if LICEcap.exe was inventoried for this computer group.
6. Click **Next Step**.
7. Name your policy and click **Create Policy**.



8. Set the **Inactive** switch to **Active**.
   - Once the policy is delivered to the endpoint agent LICEcap.exe will require the user to enter a justification reason for running this application:
   - Once the reason is entered by the user, the user clicks Continue to forward to the request to Privilege Manager for approval. On their desktop the Application Notice approval status is marked as Pending.
   - Finally, a Privilege Manager user will approve this application request

To Approve Requests

1. Return to the Privilege Manager Dashboard and navigate to **Admin: Tools | Manage Approvals**.



2. Select the approval requested from the list and click on **Approve**.
3. Select **One Time or an allotted time frame for access** and **Manage Approve**.
4. You can now return to the desktop where the user initiated the executable, and you will see the request has been approved.
5. Click on **Continue** and the user is allowed to run that executable.

> **Note:** To adjust this policy to apply to specific users or endpoints, use the option to add Inclusion/Exclusion filters and Computer Groups.

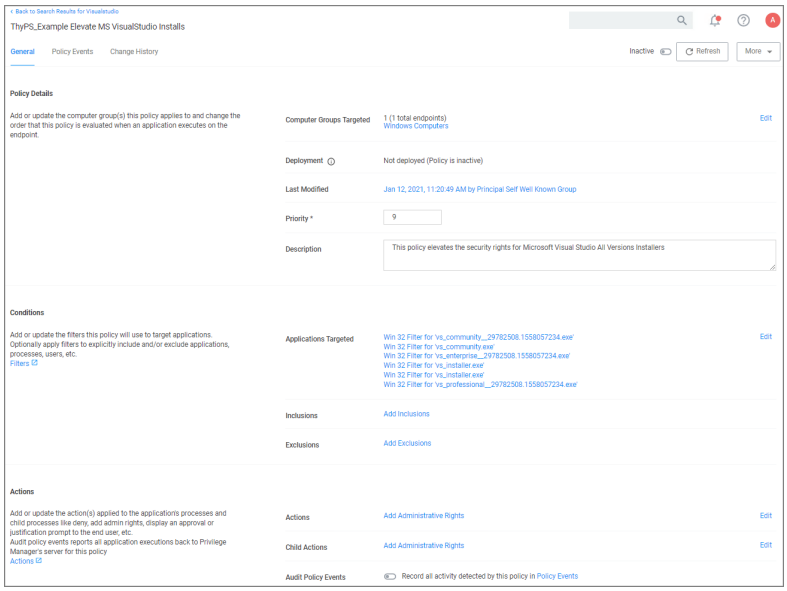
MS Visual Studio Installations

After downloading the Visual Studio Installer Elevation configuration feed, follow the below best practices to elevate Visual Studio Installer packages.

Customizing the Policy

1. In the Privilege Manager console search for **ThyPS_Example Elevate MS VisualStudio Installs**.
2. On the results page click the **ThyPS_Example Elevate MS VisualStudio Installs** policy.

Computer Groups



The policy

- is set to a priority of 9.
- incorporates various filters, covering various Visual Studio versions. Each File Specification Filter incorporates a Certificate Filter for the signing cert and a Win 32 Filter for the targeted file attributes.
- adds Administrative Rights to each of the application targets.

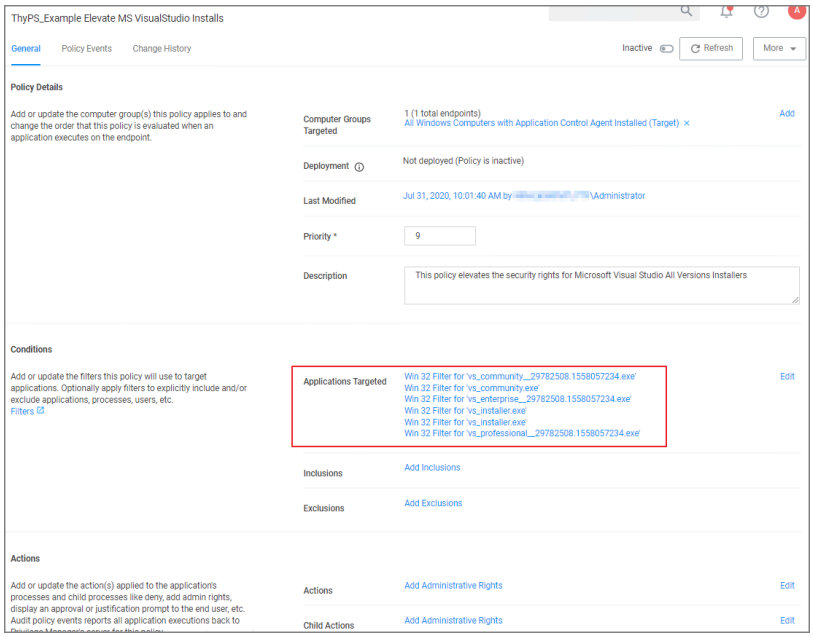
3. Save any changes and set the policy to active for it to take effect.

> Any changes to the default policy or filters will be overwritten if the configuration feed is reinstalled or updates. Delinea recommends to save items from configuration feeds that are being customized under a new name.
>
> For enhanced security, the policy should include a certificate filter when rolled out into a production environment.

Best Practices

Four Microsoft Initial download files and subsequent two Windows Start Menu target files are defined as Application targets in this default policy.

Computer Groups



If you use this policy in your environment, check frequently to update when new versions are released. Verify if there are any versions of Visual Studio you would need to include for your customization. To cover additional versions, use these filters as a basis and download desired versions including signature certificates from Microsoft. If you make changes to the default policy, take action to prevent accidental overwriting your changes when updating via configuration feed. Save the policy under a new name and compare with any Delinea provided updates in the future.

Additionally, work is needed to sort out what needs elevation when using the application's various modules. Not every module installation was tested with these filters.

The Applications Elevation Policy should be a separate Policy, as it should be located differently in the Policy Stack.

Prior to rolling this out to a production environment, proper testing by a developer should be performed.

Elevate MSI Files on the Network Share

A wizard generated UNC or Network Share Path Elevation Policy elevates .exe files but not .msi files.

When launching an .msi file, the following command line is executed:

```
C:\Windows\System32\msiexec.exe /i "\\[path-to-network-share]\[file]"
```

This means that the application is not elevated because the msiexec.exe file is not in the elevated Network Share directory.

This topic details two options for elevating .msi files from a network share.

Option 1

In order to enable elevation for .msi files on the network share, a command line filter can be created and added to the Elevation Policy.

1. In the Privilege Manager, navigate to **Admin | Filters**.
2. Click **Add Filters**.
3. From the **Platform** pull-down menu, select **Windows**.
4. From the **Filter Type** pull-down menu, select **Commandline Filter**.
5. Give this filter a custom name and description.
6. Click **Create**.
7. Under **Settings | Match Type**, select **Partial Match**.
8. In the Command line field, enter the network share path that needs to be elevated (such as `\\share\folder_path`).

9. Click **Save Changes**.
10. Navigate to your Elevation Policy. Under **Conditions** for **Application Targets** add the command line filter you just created.

Now MSI files in the network share will be elevated.

Option 2

An application control policy can be created that targets "msiexec.exe" and uses a secondary file filter as an include only filter.

1. Navigate to **Computer Groups | Windows Computers**.
2. Select **Application Policies**.
3. Click **Create Policy**.
4. In the policy wizard select **Controlling**, click **Next Step**.
5. In the policy wizard select **Elevate**, click **Next Step**.
6. In the policy wizard select **Run Silently**, click **Next Step**.
7. In the policy wizard select **Installer Packages**, click **Next Step**.
8. In the policy wizard select **File Upload**.
   a. On the Upload a File modal, Click **Choose File**.
   b. Select the file(s) you wish to be targeted.

c. Click **Upload File**.

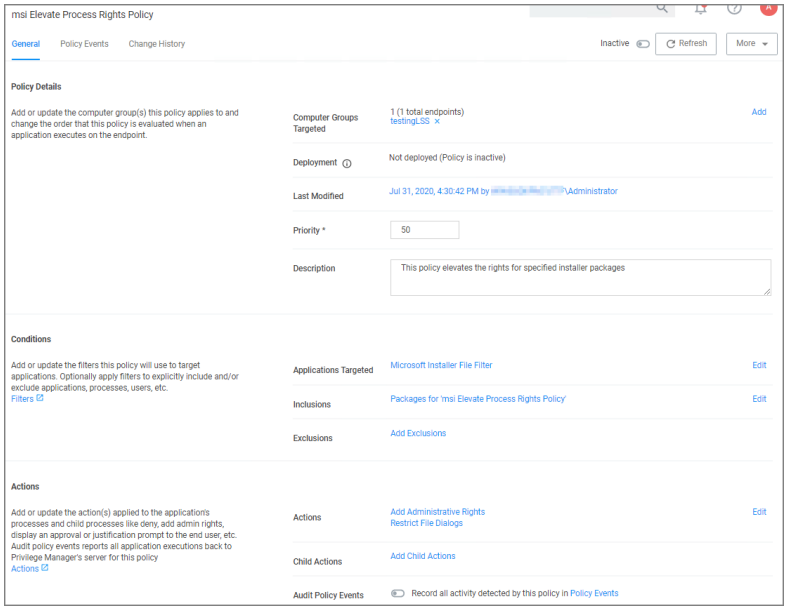
d. On the Manage Application dialog, check **File Name**.

e. Click **Create Filter**.

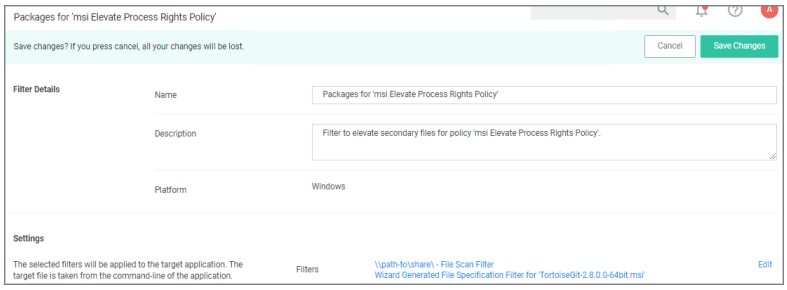
f. Click **Next Step**.

9. On the Finalize the Policy page, enter a name for your new policy. The policy will be created with a default priority of 50, since it is a silent elevation policy.

10. Click **Create Policy**.



11. Click the **Packages for 'msi Elevate Process Rights Policy'** Filter and under **Settings** search for and add the **\share\to-path** filter previously created.



12. Click **Save Changes**.

13. Set the **Inactive** switch to **Active**.

MSI files in the network share will be elevated.

Adding the Secondary File Filter created to the Applications Targets under Conditions of the Policy will catch all instances where `.msi` files are run from `\\share\folder_path`. Only msiexec.exe will run .msi files, so the Secondary File Filter can be added to an Elevation Policy that has other Application Targets.

An Elevation Policy can be built with this Secondary File Filter as the Application Target and add the built-in Microsoft Installer File Filter as an Inclusion Filter to specifically target msiexec.exe runs an .msi from `\\share\folder_path\`.

Network Share Applications

Many organizations put trusted installers on a network share that employees can use. Those installers can be elevated automatically from the shared network location by assigning an elevation policy to the network share location.

There are different options to elevate rights to launch applications from a network share location.

- One option is to create a file specification filter setting the path for the network share location. Then use that filter in a policy to apply administrative rights to all application launches from that path.
- The other option is to download the Application Control - UNC Elevation Policy Template via Config Feeds and customize the template.

Applying Administrator Rights to a Network Share

Creating the Filter

1. In the Privilege Manager Console navigate to **Admin | Filters**.
2. On the Filter page, click **Create Filter**.
3. On the New Filter page, select the platform. This can be either **Both Windows / macOS**, **Windows**, or **macOS**. For this example, select **Windows**.
4. From the **Filter Type** drop-down select **File Specification Filter**. This also allows you to link in hashes or signatures.
5. Enter the name and a description for the filter, for example "network share" and "filter to elevate applications installed from network share".
6. Click **Create**.
7. Add the Path that points to your Fileshare folder, click **Save Changes**. Use the same UNC path format for both macOS and Windows endpoints.

Creating the New Policy

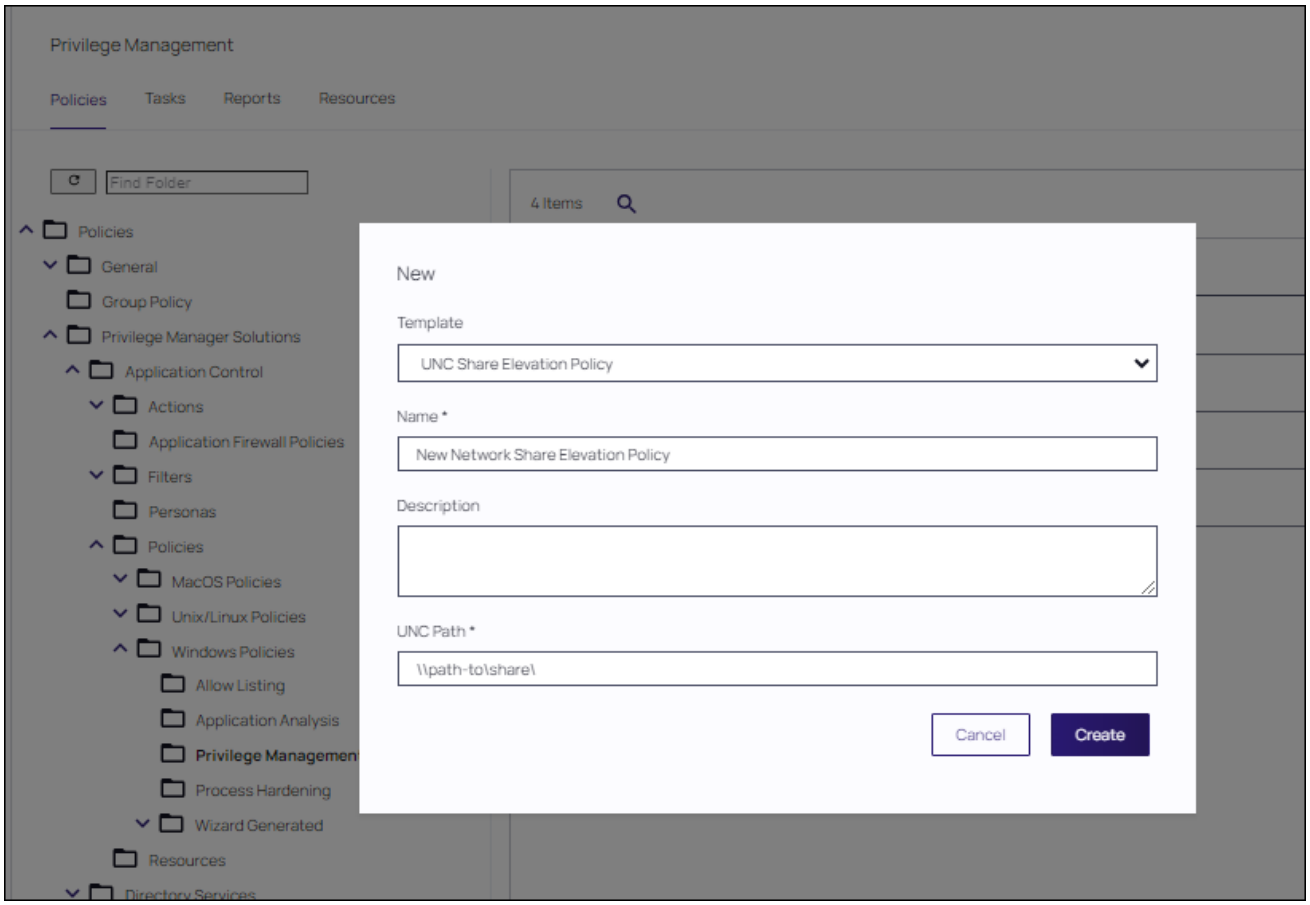
1. Navigate to **Computer Groups | Windows Computers**.
2. Select **Application Policies**.
3. Click **Create Policy**.
4. In the policy wizard select **Controlling**, click **Next Step**.
5. In the policy wizard select **Elevate**, click **Next Step**.
6. In the policy wizard select **Run Silently**, click **Next Step**.
7. In the policy wizard select **Installer Packages**, click **Next Step**.
8. In the policy wizard select **Existing Filter**.

9. Search and add the network share path filter previously created.
10. Click **Update**.
11. Click **Next Step**.
12. Name your policy and enter a description.
13. Click **Create**.
14. Set the **Inactive** switch to **Active**.

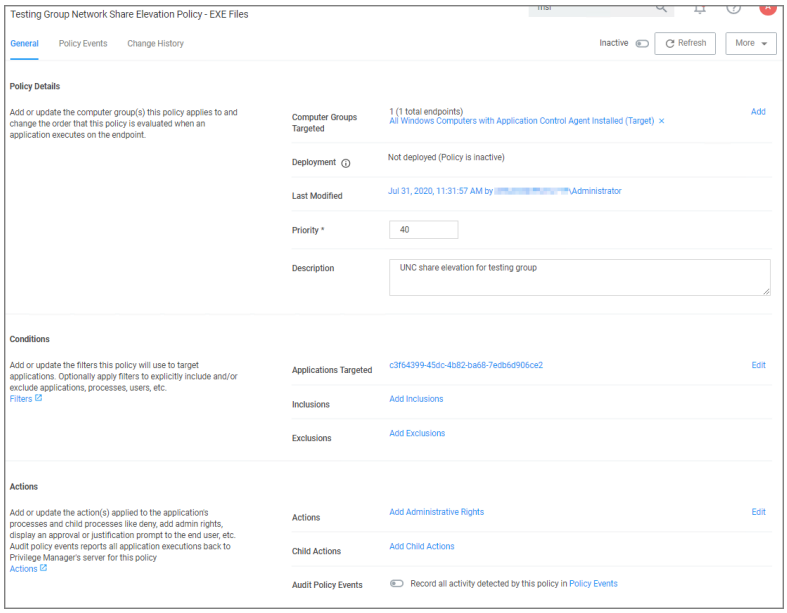
Using the UNC Elevation Policy Template

Use the UNC Elevation Policy Template to create a customized policy that lets you scan a network share and automatically elevates launches of MSI and EXE files from that share.

1. Navigate to **Admin | Config Feeds**.
2. Expand **Privilege Manager Product Configuration Feeds**.
3. Expand **Application Control Solution**.
4. Locate the **Application Control - UNC Elevation Policy Template** and click the **Install** link. The template is installed.
5. Navigate to **Admin | Folders**.
6. In the folder tree open **Privilege Manager Solutions | Application Control | Policies | macOS or Windows policies | Privilege Management**.
7. Click **Create**.
8. From the template drop-down select **UNC Share Elevation Policy**.
9. Enter a name and description.
10. Enter the UNC Path to the network share. Use the same UNC path format for both macOS and Windows endpoints.



11. Click **Create**.
12. The Policy is created, but needs some attention. Confirm that this is an elevation policy and click **Set as Elevate**.



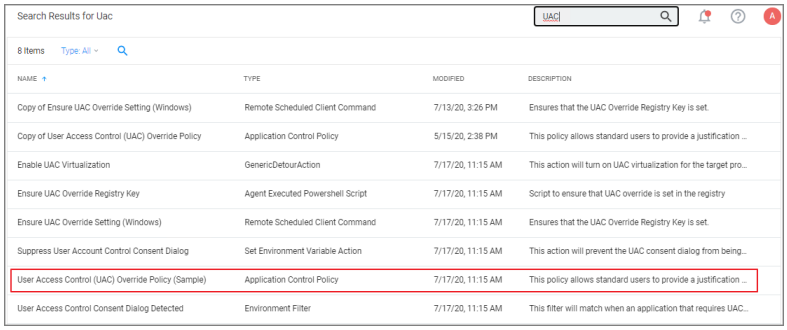
13. Change the priority based on how this policy needs to interact with other policies for your organization, click **Save Changes**.
14. Set the **Inactive** switch to **Active**.

UAC Override Policy

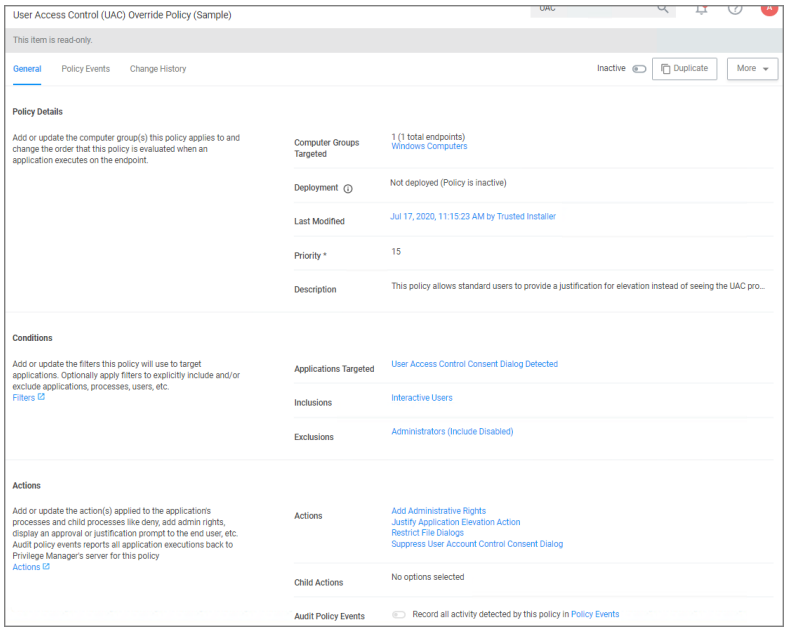
By creating a User Access Control (UAC) Override Policy you can override UAC prompts for end-users. You can create custom messages that require users to submit a reason for requesting administrator rights, which replace UAC prompts for credentials.

Using the Default Policy

1. Under **Computer Groups** search for **User Access Control (UAC) Override Policy (Sample)**.



The UAC Override Policy is a read-only item, that allows standard user to provide a justification for elevation instead of seeing the UAC prompt.



2. To edit this policy, you need to make a copy and assign a different name, to do so click **Duplicate**.
3. Under **Computer Groups Targeted** you may change the targeted endpoints.
4. Under **Conditions** you edit the
   - Application Targets
   - Inclusion Filters
   - Exclusion Filters
5. Under **Actions** you can edit
   - the available actions for the policy like
     - the Justify Application Elevation Action
     - the Add Administrative Rights Action
     - the Suppress User Account Control Consent Dialog (Legacy) Action. Only used with Agent versions 10.4 and older.
   - if you want to Audit Policy Events (as a learning mode/monitoring feature)
   - you can add Child Actions.
6. Click **Save Changes**, if you created a copy and made edits.
7. Set the **Inactive** switch to **Active**.

By default the UAC Override Policy has a priority setting of 15.

Targeting MSI

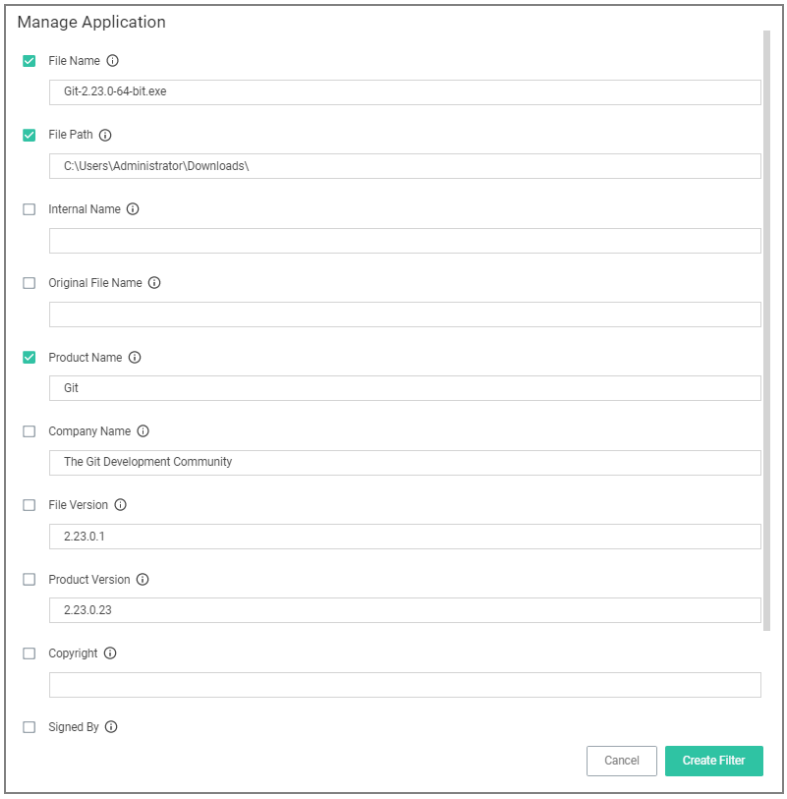
1. Create a new elevation policy that targets the **MSIElevateHost.exe** application. Other filters can be added to target a secondary MSI file or command if desired, but it is not required.

2. Add the **Add Administrator Rights** action; as well as one of the message actions such as Justification or Approval.

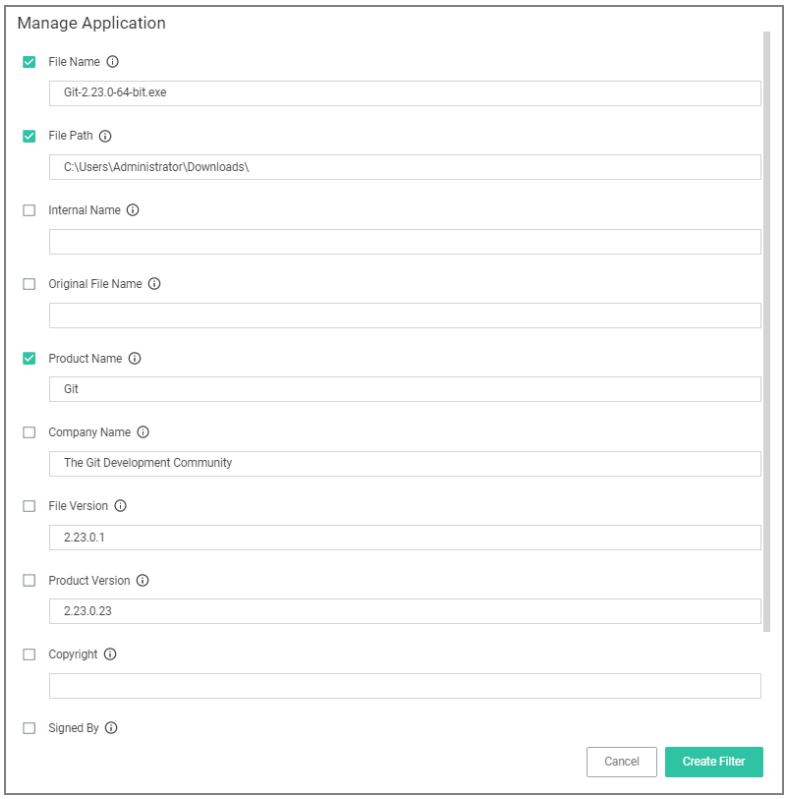
User Justification Required to Run

This policy type requires a user to provide a justification for why they need to run an application before elevating with administrator privileges. User Justification refers to the policy action. Since Conditions and Actions are independent, this action can be applied to any condition. In this use case, we will simply apply this action to a specific application.

1. Using the Policy Wizard, create a controlling policy that elevates application execution on endpoints.
2. Select **Require Justification**, and click **Next Step**.
3. Select what file type to target, for this example select **Executable**, and click **Next Step**.
4. Choose your target, for this example **File Upload**.
5. Click **Choose File** and select a file to upload.
6. Click **Upload File**.
7. On the **Manage Application** page select all the identifying factors you want the filter to target.



8. Click **Create Filter**.
9. Click **Next Step**.
10. Name your policy and add a description, click **Create Policy**.



11. Set the **Inactive** switch to **Active**.

The user will see a justification message as a result of the policy. When the user adds a reason, they will then click the **Continue** button and the application is allowed to execute.

> **Note:** You can then view a user's provided reasons in Privilege Manager under **Reports | Application Justification Summary Details Report**.

Monitoring Policies

Monitoring Policies apply to any unknown applications that will attempt to run in your environment. It is important to discover unknown applications and determine whether to let them run or whether they are harmful. Monitoring provides a system for discovering the unknowns and adding an action that hinges on a reputation check.

To discover these applications, for example, applications in a user's environment that are currently requesting or using elevated permissions, open the policy in question and click the **Policy Events** tab.

The following examples are available:

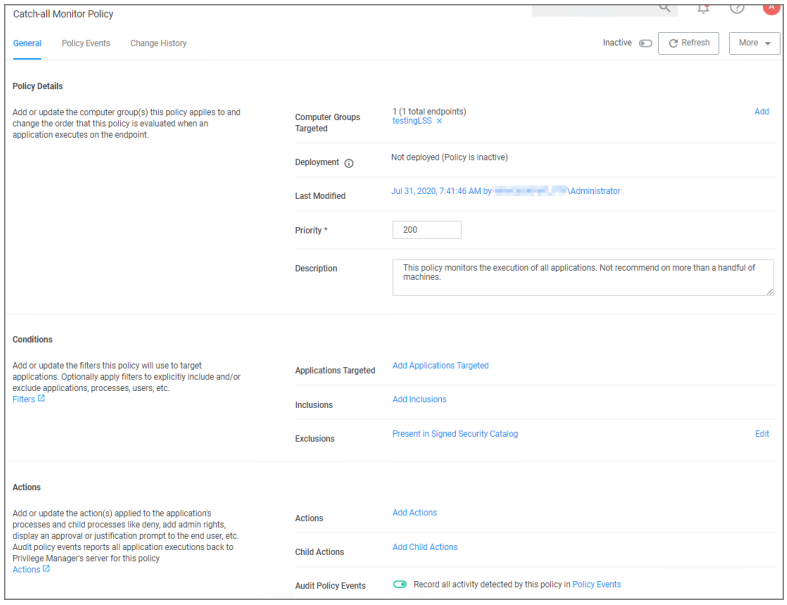
- Catch-All Policy
- Reputation Checking

Catch-All Policy

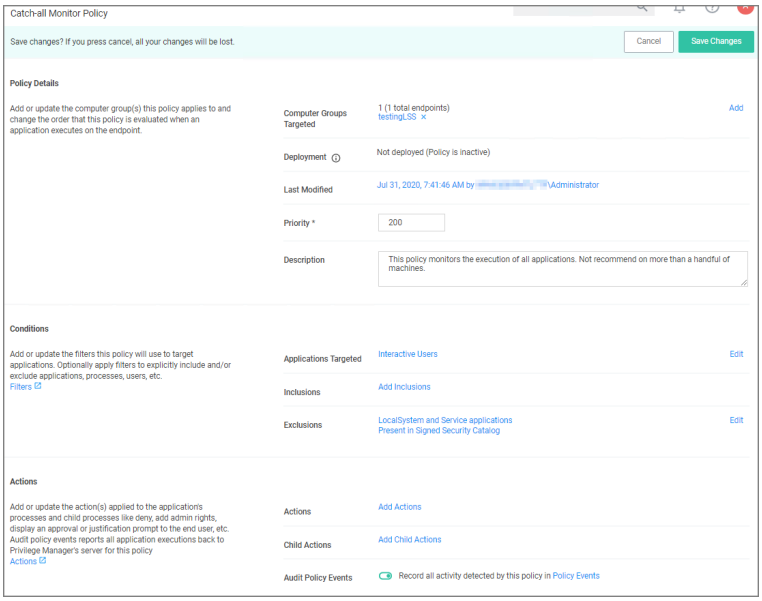
A useful Learning Mode Policy to set up in Production environments is called a Catch-All Policy. This type of policy will gather information on any executables in your environment that are not satisfied by other Privilege Manager policies.

Note: These types of Catch-all monitor policies SHOULD NOT BE used for the Windows or macOS Computer Groups. Those groups apply to ALL computers in the environment and unless a monitor policy like this is setup to work with really good allow policies in front a lot of events will be sent.

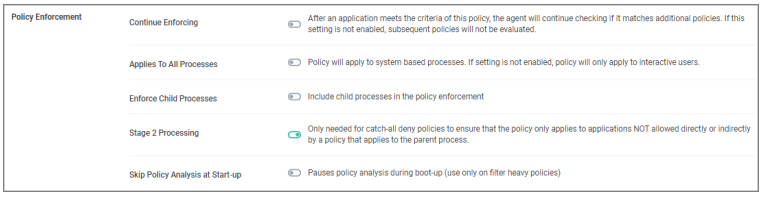
1. Under your Computer Group for which you want to monitor all activities select **Application Policies** and click **Create Policy**.
2. From the Policy Wizard select **Monitoring** and click **Next Step**.
3. Select **Everything** and click **Next Step**.
4. Enter a name, for example *Catch-all Monitor Policy*.
5. Click **Create Policy**.



6. Customize the policies Conditions, Actions, and Policy Enforcement, for example:
   - Under Applications Targeted, click **Add Application Target** and search for and add **Interactive Users**.
   - Under Exclusions, click **Edit** and add **LocalSystem and Service applications** to the exclusion list.



- Under **Show Advanced | Policy Enforcement** set the switch for **Stage 2 Processing** to active an all others to inactive.



7. Click **Save Changes**
8. Set the **Inactive** switch to **Active**.

Reputation Checking

Privilege Manager analyzes applications in real-time. This unique feature allows for reputation analysis of any unknown applications that will mitigate endpoint attacks from Ransomware, Zero-day attacks, Drive-by Downloads, and other unknown malicious software.

The monitor approach used here is that all applications that meet a general condition (i.e. executed from a specific directory or directories) will be sent to VirusTotal for a reputation check. For this use case we will perform real-time reputation analysis of unknown applications using VirusTotal.

First, you will need to integrate Privilege Manager and VirusTotal by following the Integration steps listed in the Setting Up VirusTotal for Reputation Checking topic. That section will walk you how to do the following:

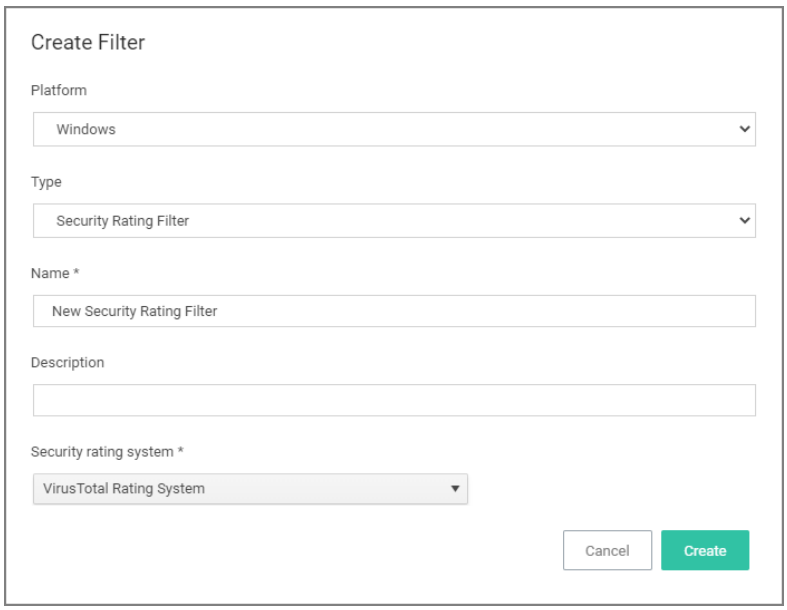
1. Configure VirusTotal Ratings Provider
2. Install VirusTotal in Privilege Manager
3. Create a Security Rating Filter for VirusTotal

For information and setup steps to configure reputation checking using Cylance, see the Cylance Integration topic.

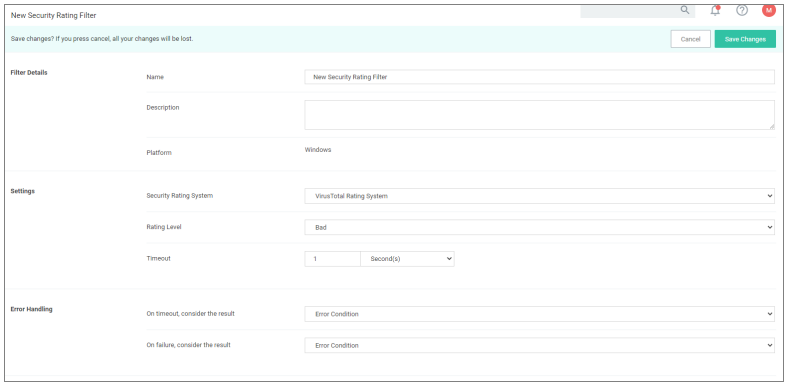
Creating Security Rating Filter

Next you have to create a Security Rating Filter for VirusTotal. Follow these steps:

1. Navigate to **Admin | Filters**, the click **Create Filter**.
2. Select a platform, then **Security Rating Filter** as a Filter Type. Name the policy and add a description.
3. From the **Security Rating System** drop-down, select **Virus Total Rating System**.



4. Click **Create**.
5. Under **Settings**, change the **Rating Level** drop-down to specify **Bad**.

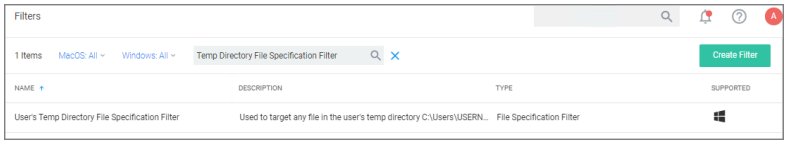


The rating level trigger is supposed to match what you want to accomplish with the policy that will be using this filter. A rating level of Bad should be used for Deny policies, and Clean for applications or files that are part of the safe list. A rating level of Suspect can be used in justification and/or learning/discovery policies.

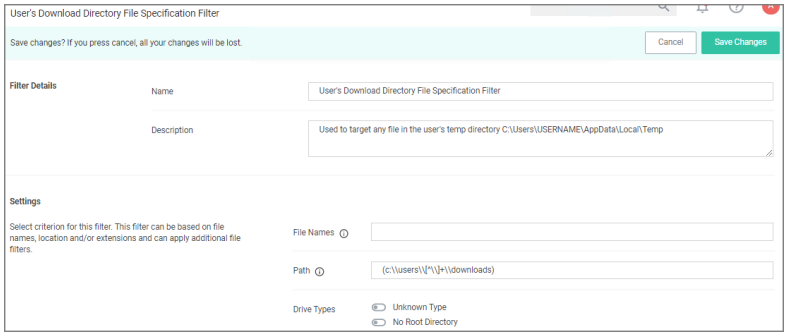
6. Click **Save Changes**.

Creating User's Downloads Location, Temp Dir, and Collection Filters

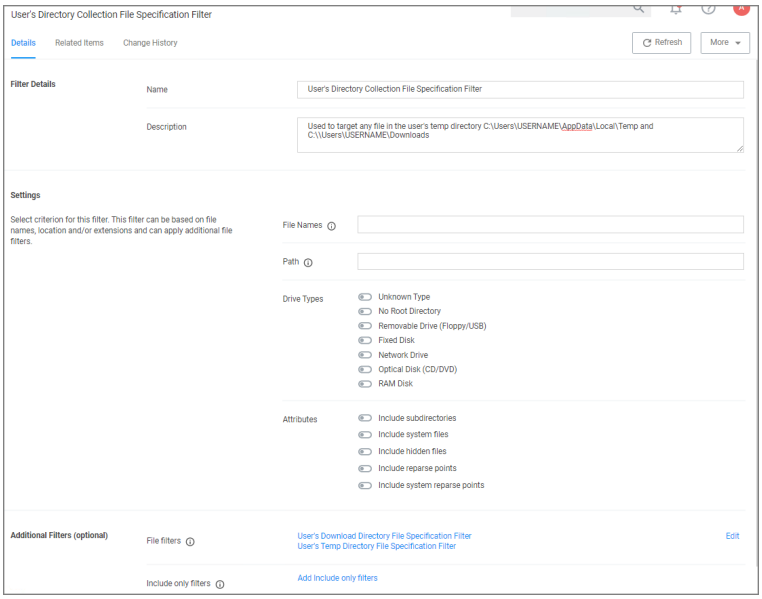
1. Navigate to **Admin | Filters** and search for **Temp Directory File Specification Filter**.



2. Select the filter **User's Temp Directory File Specifications Filter**, click **Duplicate**.
3. Name the new filter *User's Download Directory File Specification Filter*, provide a description and click **Create**.
4. Change the regular expression in the Path filed to the following: (c:\\users\\[^\\]+\\downloads).



5. Click **Save Changes**.
6. Finally, combine the 2 filters into a single filter to target both directories.
   a. Click **More | Duplicate**.
   b. Enter the name for the new filter *User's Directory Collection File Specification Filter*, click **Create**.
   c. Clear the data in the Path field.
   d. Under Additional Filters, click **Add File filters**.
   e. Search for **User's Download** and add the **User's Downloads Directory File Specification Filter**.
   f. Search for **User's Temp Directory** and add **User's Temp Directory File Specification Filter** (this is a default filter).
   g. Click **Update**.

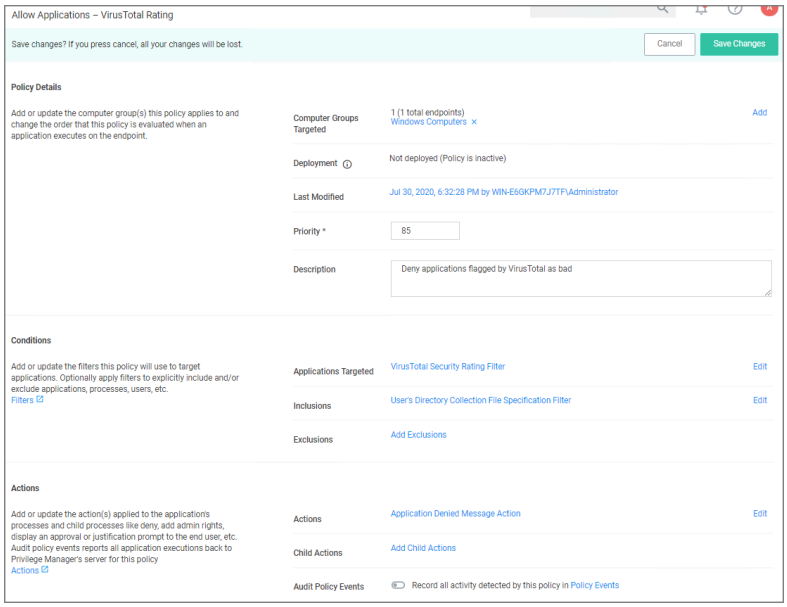


h. Click **Save Changes**.

Creating a Policy

Next you have to create a Policy and add the filters for VirusTotal:

1. Using the Policy Wizard, create a controlling policy that allows application execution on endpoints.
2. Select **Existing Filter**.
3. Search for add the previously created **VirusTotal Security Rating Filter**.
4. Click **Update**
5. Name the policy **Allow Applications - VirusTotal Rating**, and add a description *Deny applications flagged by VirusTotal as bad*, click **Create Policy**.
6. Click **Add Inclusions**, search for and add the **User's Directory Collection File Specification Filter**.
7. Click **Update**



8. Click **Save Changes**.
9. Set the **Inactive** switch to **Active**.

> **Note:** This policy will send any application run from the user's Downloads or Temp directory to VirusTotal for a reputation check in real-time. If the application is graded with Bad from VirusTotal, the application will be denied.

Viewing a File Security Ratings Report

To view a File Security Ratings report, search for **File Security Rating Details Report**. To see details of the applications in the report, click on the file name in the File column.

Allow Listing Policies

Allow listing is a type of policy that allows applications to run on your endpoints. You can think of allow listing as a neutral policy type because it does not alter an application's default permissions, it merely signifies that the application is “known/trusted” and allowed to run. Although simple allow listing follows normal, user-level credentials, allow listed applications are also often paired with Elevation Policies outlined Elevation Policies.

The following examples are available:

- Allow MS Security Catalog
- Allow Google Application with File Upload

Allow Listing Policies without Actions

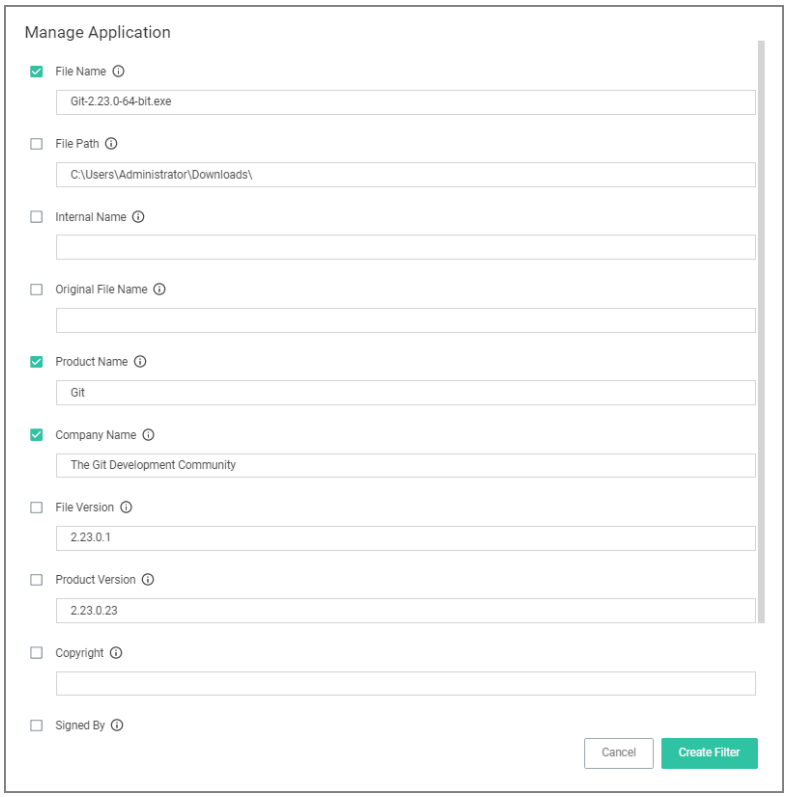
If an application is allow listed under a user context instead of group context and without an action specified, Delinea recommends to use the Administrators (Include Disabled) filter for the policy to execute as desired.

Git App with File Upload

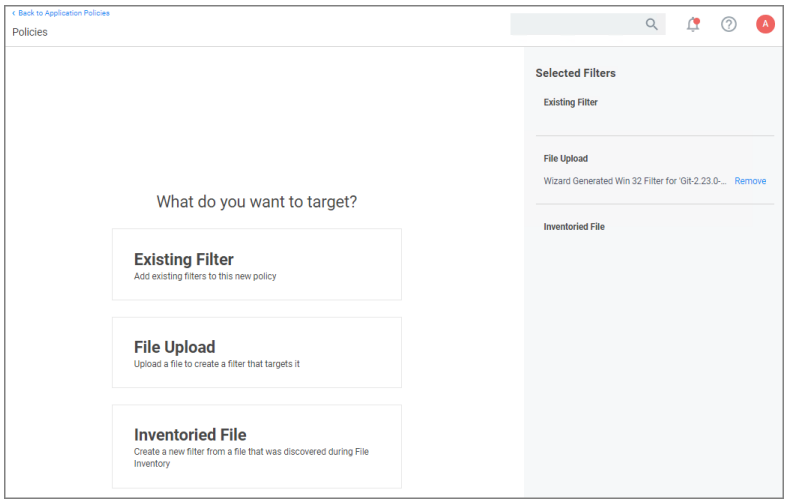
In evaluation and production installations, proactive introduction of executables into Privilege Manager can be accomplished with a feature called File Upload. File Upload allows you to quickly introduce a file, then create a Filter and/or a Policy to govern the application. As example, here's how to introduce the Git Installer into Privilege Manager and use the file information to allow list Git applications.

For this use-case you will need to have access to downloaded Git installer files.

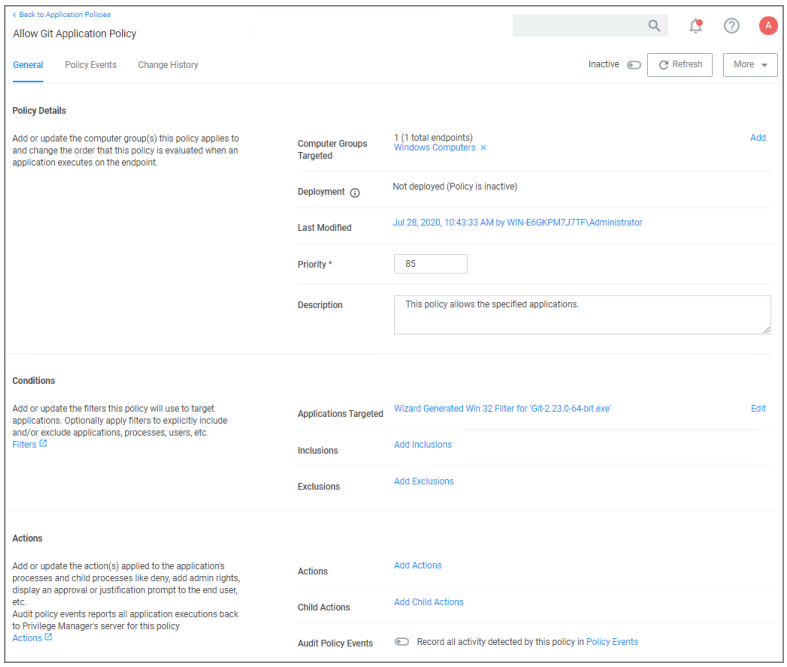
1. Using the Policy Wizard, create a controlling policy that allows application execution on endpoints.
2. Select what process types you want the policy to allow, for this example it's **Specific Applications**.
3. Choose your target, for this example **File Upload**.
4. Click **Choose File** and select a file to upload.
5. Click **Upload File**.
6. On the **Manage Application** page select all the identifying factors you want the filter to target.



7. Click **Create Filter**.



8. Click **Next Step**.
9. Name your policy and add a description, click **Create Policy**.

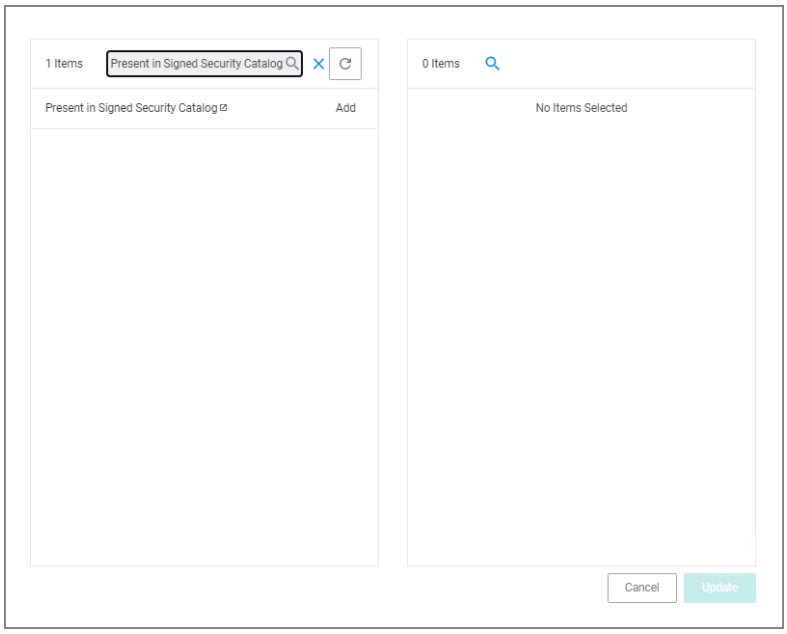


10. Set the **Inactive** switch to **Active**.

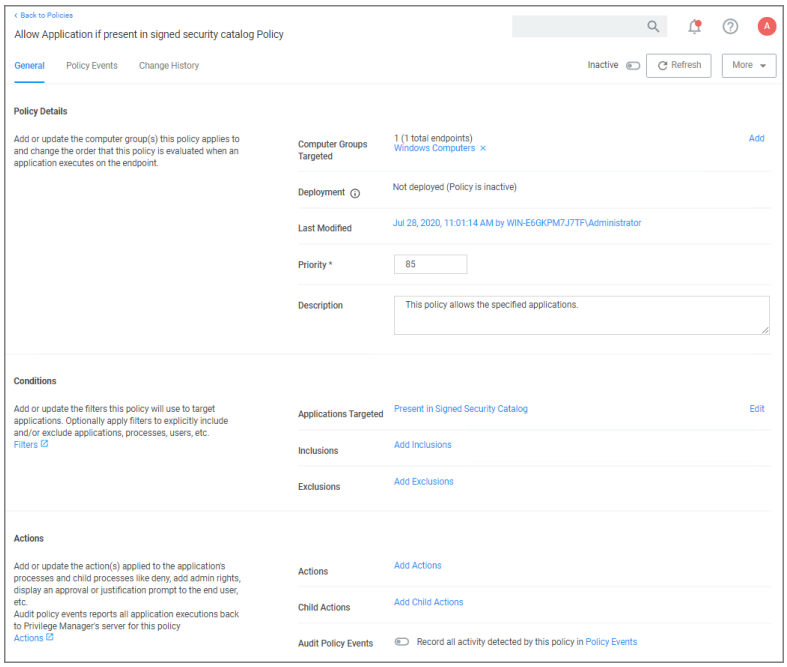
MS Security Catalog

This policy uses a built-in filter to allow list Microsoft's Signed Security Catalog. This filter is often used to dynamically allow to update items from Microsoft. Allow listing these executables clears them so they are not effected by any other policy, (i.e. they are allowed to run).

1. Using the Policy Wizard, create a controlling policy that allows application execution on endpoints.
2. Select what process types you want the policy to allow, for this example it's **Specific Applications**.
3. Choose your target, for this example **Existing Filter**.
4. Search for and **Add** the **Present in Signed Security Catalog** filter.



5. Click **Update**.
6. Click **Next Step**.
7. Name your policy and add a description, click **Create Policy**.



8. Set the **Inactive** switch to **Active**.

There is no need to add actions under the Actions tab, because these applications are allow listed, they are allowed to run with default permissions.

Platform-Specific Policies

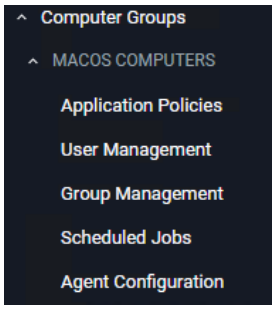
Policies for monitoring and controlling each default computer group that are specific to each platform are presented in this section, along with examples and links to the policy wizard.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

The wizard provides on page help explaining the different options available to the user.

macOS Computers

The default macOS Computer Group is the navigation entry point into the macOS Computer Group. The sub nodes are in feature parity with other OS computer groups. All policies or resources underneath **MACOS COMPUTERS** pertain to that specific default computer group.



Refer to the Policy Wizard section for details on decision points for:

- Creating a Monitoring Policy

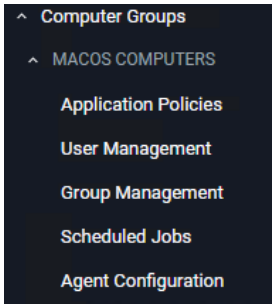
The following macOS controlling policy decision diagrams are available:

- Creating a Controlling Elevation Policy for macOS
- Creating a Controlling Allow Policy for macOS
- Creating a Controlling Block Policy for macOS

For macOS Agent Configuration information refer to Agent Configuration.

macOS Computers

The default macOS Computer Group is the navigation entry point into the macOS Computer Group. The sub nodes are in feature parity with other OS computer groups. All policies or resources underneath **MACOS COMPUTERS** pertain to that specific default computer group.



Refer to the Policy Wizard section for details on decision points for:

- Creating a Monitoring Policy

The following macOS controlling policy decision diagrams are available:

- Creating a Controlling Elevation Policy for macOS
- Creating a Controlling Allow Policy for macOS
- Creating a Controlling Block Policy for macOS

For macOS Agent Configuration information refer to Agent Configuration.

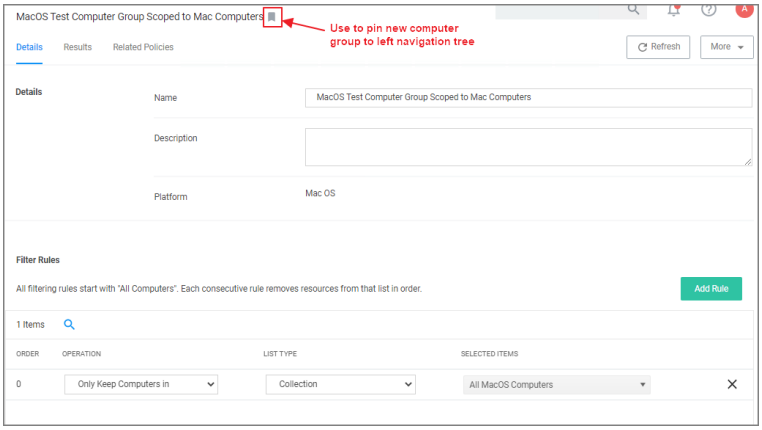
Adding macOS Agents to a Computer Testing Group

The Policy Configuration examples in the following section will use a Learning Mode Policy that enables us to perform actions (i.e. run applications) on a test computer that Privilege Manager will then pick up. This makes targeting specific applications during policy creation easy.

Creating a macOS Test Computer Group

To create a Monitoring (or Learning Mode Policy) on your Mac, begin by

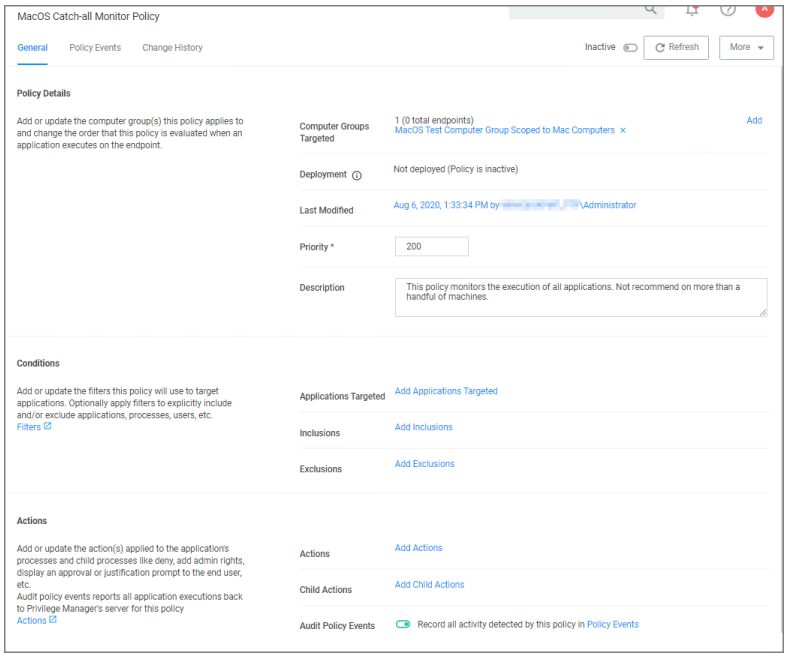
1. Creating a macOS based test computer group:
   a. Navigate to **Computer Groups**.
   b. Click **Create Computer Group**.
   c. From the **Platform** drop-down select macOS.
   d. Enter a name and description for your new group.
   e. Click **Create**.



   f. Add the macOS endpoints you want to be part of the computer group.
   g. Click **Save Changes**.
   h. Pin your computer group to the left navigation menu for quick access. Click the bookmark icon next to the computer group name.

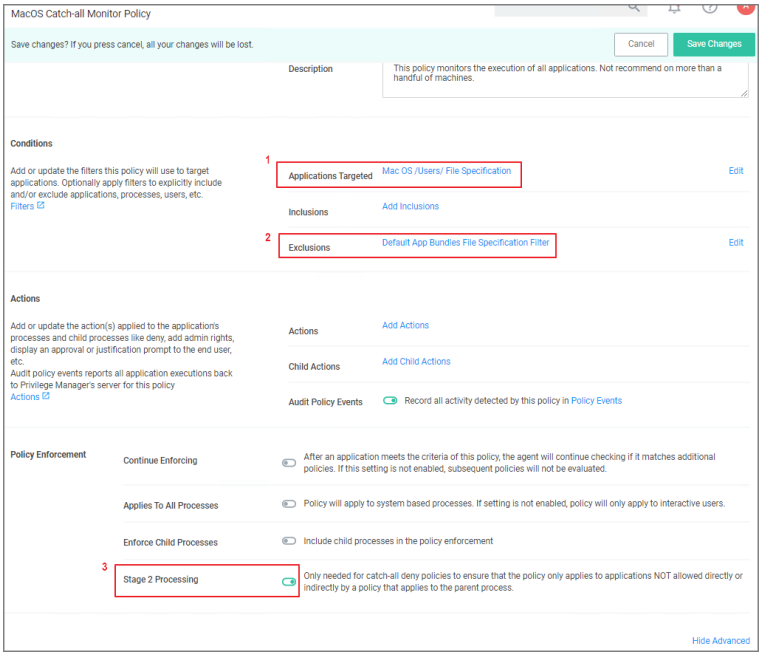
Setting Up Monitoring Policies for macOS

1. Under your macOS Test Computers Computer Group select **Application Policies** and click **Create Application Policy**.
2. From the Policy Wizard select **Monitoring** and click **Next Step**.
3. Select **Everything** and click **Next Step**.
4. Enter a name, for example *macOS Catch-all Monitor Policy*.
5. Click **Create Policy**.



6. Customize the policies Conditions, Actions, and Policy Enforcement, for example:
   - Under Applications Targeted, click **Add Application Target** and search for and add **macOS/Users/File Specification**.
   - Under Exclusions, click **Edit** and add **Default App Bundles File Specification Filter** to the exclusion list.
   - Under **Show Advanced | Policy Enforcement** set the switch for **Stage 2 Processing** to active an all others

to inactive.



7. Click **Save Changes**
8. Set the **Inactive** switch to **Active**.

This "Testing Computers" group should only be used for testing specific machines and configuration purposes. It should not be assigned to large groups of computers in your production environment.

Verify that under **Actions** the **Audit Policy Events** switch is active.

Request Application Installation

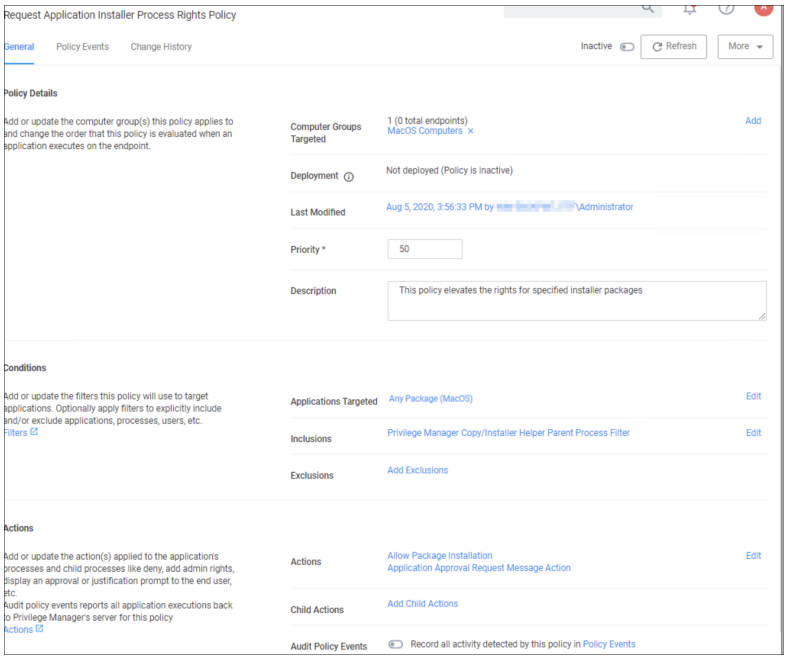
Note: This is the procedure for the kernel extension.

Privilege Manager can allow macOS users to install packages on demand. Do the following to create a policy to allow users to request installation of certain packages. For this to work, your endpoint must be online. If the system is offline, refer to the Offline Approval process documentation.

1. Navigate to your macOS Computer Group and select **Application Policies**.
2. Click **Create Policy**.
3. Select **Controlling** and click **Next Step**.
4. Select **Elevate** and click **Next Step**.
5. Select **Require Approval** and click **Next Step**.
6. Select **Installer Packages** and click **Next Step**.
7. Select what exactly you want the policy to target. This can be based of an **Existing Filter**, a **File Upload**, and/or **Inventoried File(s)**. Multiple targets can be selected. Our example shows the **Any Package (macOS)**. Click

Next Step.

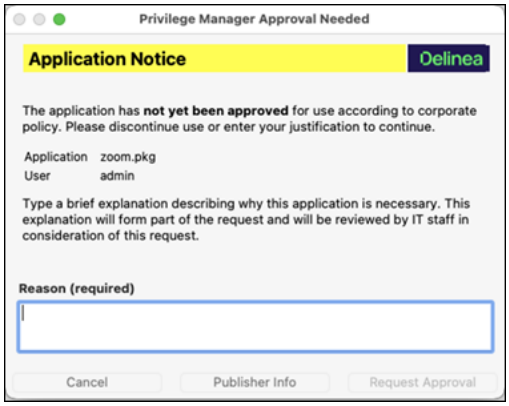
8. Enter a Name and description for your policy, click **Create Policy**.



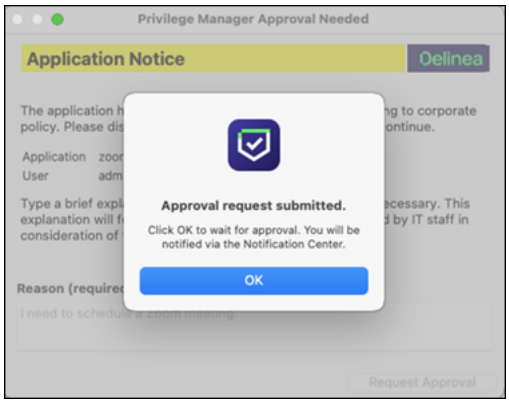
9. Set the **Inactive** switch to **Active** for policy updates at the endpoint.

Once the policy is enabled and in place at the endpoint, a user will typically go through the following steps to request an application installation:

1. When clicking on a pkg file, the following Application Notice opens:



2. Enter the Reason why the application should be installed and click the Request Approval button. The **Approval request submitted.** dialog opens.



3. You will be notified of any status change via the notification center. Click **OK** to wait for the approval.

macOS Application Approval Process via Sudo Plugin

The macOS sudo plugin provides the means to run an application elevated via Terminal.app on macOS systems running Catalina or newer macOS versions and the SYSEX Privilege Manager agent on the workstation. The sudo plugin also provides user feedback via Terminal when the request is approved or denied.

When an application policy requires approval, the user will initially be presented with the defined approval action text along with the following message in Terminal `Enter your response, or type Ctrl+D to cancel:`, this allows the user to cancel out of the approval process and the command will not be run. For the approval workflow, the user has to enter a response text for the approval. Once the approval has been submitted the user is presented with a message in Terminal `Waiting for approval... (Ctrl+C to cancel)`. The application execution is blocked until the approval comes in. If the request is approved, the application runs. If it is denied, the process exits. If the user cancels, the command will not run.

Note: Not supported on endpoints running the KEXT agent.

Example: Elevate systemsetup Command

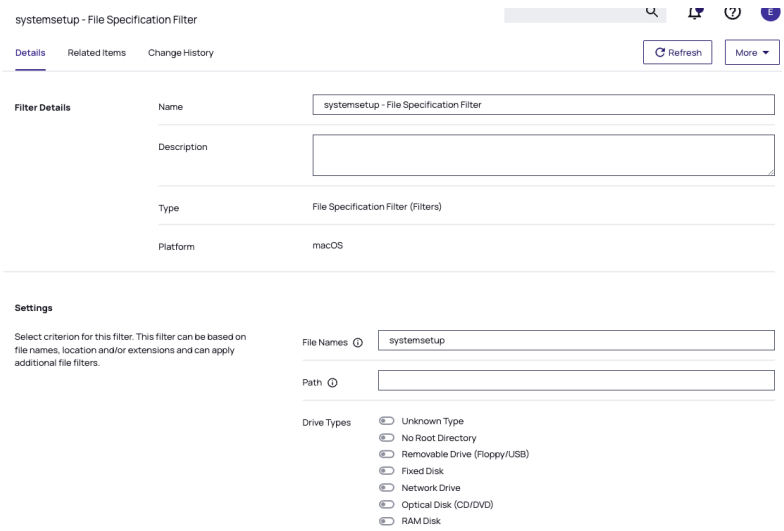
The following policy is configured to elevate the `systemsetup` command after an approval when run via `sudo`.

Create a systemsetup File Specification Filter

This filter will specify the applications targeted.

1. Navigate to **Admin | Filters**.
2. Click **Create Filter**.
3. From the Platform drop-down, select **macOS Computers Filters**.
4. From the Type drop-down under **File Filters (macOS)**, select **File Specification Filter**.
5. Name the filter and provide a description to reflect the purpose, for example *systemsetup - File Specification Filter*.
6. Click **Create**.
7. Under **Settings | File Names**, enter **systemsetup**.

8. Click **Save Changes**.

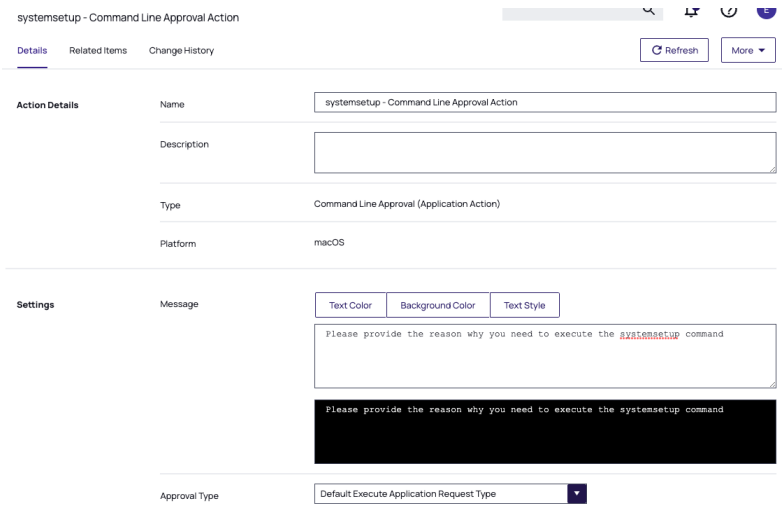


Creating the Command Line Approval Action

This action will be added under the Actions section of the policy.

1. Navigate to **Admin | Actions**.
2. Click **Create Action**.
3. From the **Platform** drop-down, select **macOS Computers Actions**.
4. From the **Type** drop-down, select **Command Line Approval Message**.
5. Name the action and provide a description to reflect the purpose, for example *systemsetup - Command Line Approval Action*.
6. Click **Create**.
7. Under **Settings | Message**, provide a message that will be displayed to the user before they are required to enter their reason, for example *Please provide the reason why you need to execute the systemsetup command*.
   a. Under Settings you can also set the Text Color, Background Color, and Text Style that is presented to the user when entering the approval process.
8. From the **Approval Type** drop-down, select **Default Execute Application Request Type**.

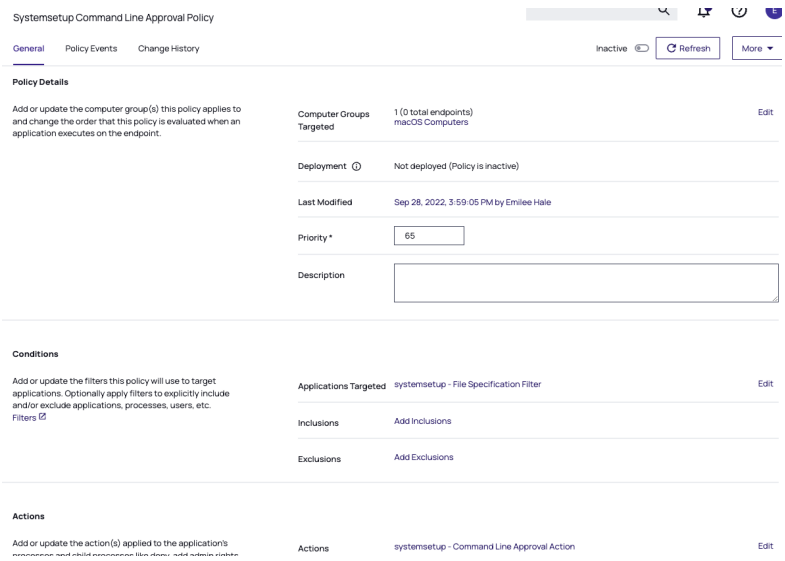
9. Click **Save Changes**.



Creating the Systemsetup Command Line Approval Policy

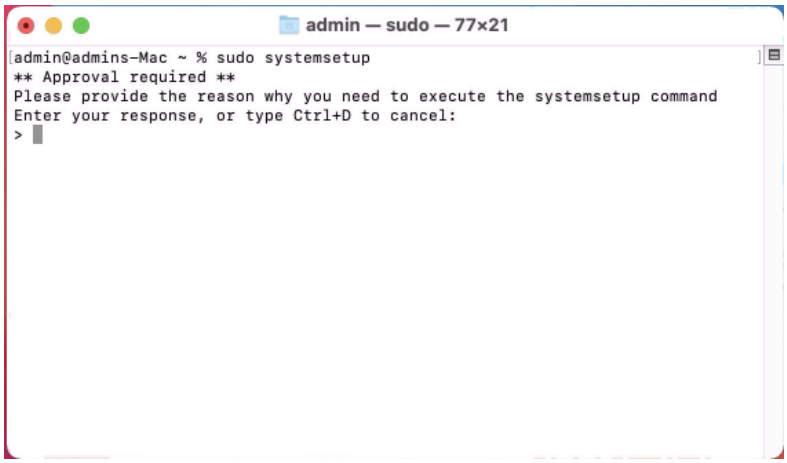
1. Navigate to your macOS computer group and select **Application Policies**.
2. Click **Create Policy**.
3. Select the option **Skip the wizard, take me to a blank policy**.
4. Name the policy, for example *Systemsetup Command Line Approval Policy*.
5. Click **Create Policy**.
6. Under **Conditions | Applications Targeted**, click **Add Application Target**.
7. Search for and add the *systemsetup - File Specification Filter* previously created.
8. Click **Update**.
9. Under **Actions**, click **Add Actions**.
10. Search for and add the *systemsetup - Command Line Approval Action* previously created.
11. Search for and add the built-in **Run as Root** action.
12. Click **Update**.
13. Click **Save Changes**.

14. Enable the Policy.



Workstation Interaction

1. At the macOS endpoint, open Terminal.app and run systemsetup via sudo. The **Approval required** message opens:



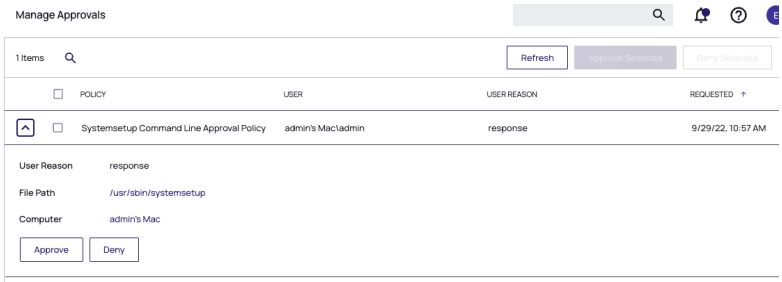
2. Enter the approval reason and hit the Enter key.

   In the Terminal, **Waiting for approval... (Ctrl+C to cancel)** is displayed and the approval request is submitted. You will be notified of any status change via the Terminal.app.

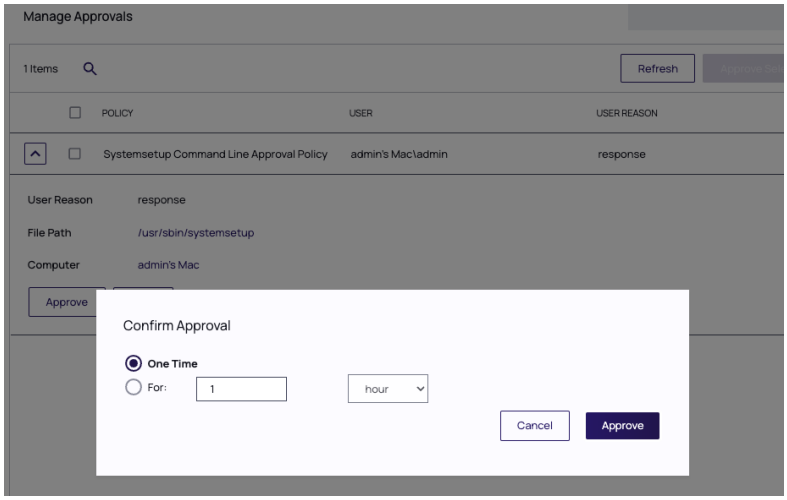
Privilege Manager Console Interaction

1. As an approval supervisor, navigate to **Admin | Manage Approvals**.

2. If no approval requests are listed, click **Refresh**.
3. **Expand** the approval you want to either approve or deny.



4. Click **Approve**.

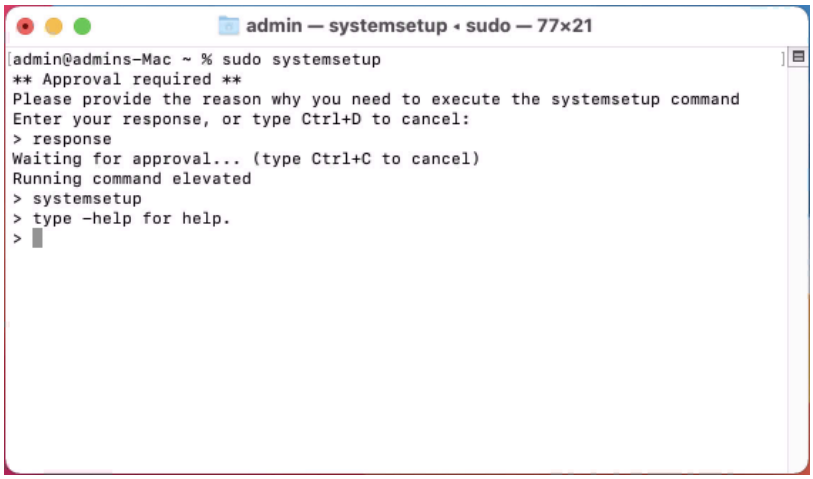


5. On the **Confirm Approval** modal, choose to either issue a **One Time** or a **timed** approval. The default opens to **One Time**.
6. Click **Approve**

Workstation Interaction

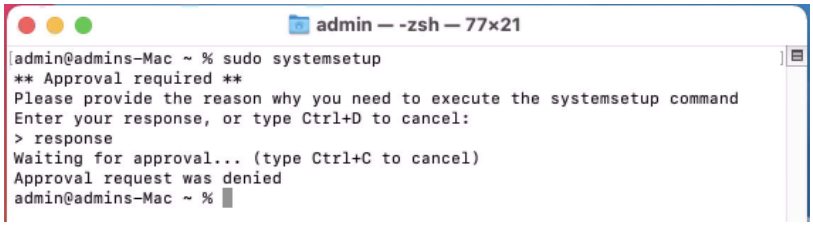
Following Approval

Following an approval, Terminal writes **Running command elevated** and shows other process messages.



Following Denial

Following a denial, Terminal writes **Approval request was denied** and shows other process messages.



macOS Approval Process

To accommodate the new macOS Endpoint Security system extensions, the approval workflow of the macOS agent now terminates any justification or approval process and presents the user with an applicable message action.

The following workflows are impacted by this change:

- Application Approval Request Message Action
- Deny Execute
- Deny Execute and Deny Execute Message Action
- Deny Execute and Application Denied Message Action
- Application Justification Message Action
- Application Warning Message Action

Refer to the Actions topic.

Application Approval Request Message Action

Workflow **prior to** Privilege Manager **v10.8**:

Action waits for the user to either click **Cancel** or enter an **Approval Request Message** and click **Request Approval**.

Workflow **starting with** Privilege Manager **v10.8**:

Privilege Manager immediately denies the execution with macOS displaying a dialog indicating the application can't be opened. If the user has granted Privilege Manager.app the necessary *SendEvents* right, Privilege Manager closes the dialog.

- If the user clicks **Cancel**, the dialog is dismissed and no further action taken.
- If the user clicks **Request Approval**, the Approval is submitted and the user is presented with a modal dialog informing them that the approval request has been submitted and that they will be notified via Notification Center.
  - If successfully submitted, the request is queued and monitored by Privilege Manager.app.
  - If denied, a notification is pushed to the Notification Center indicating the app was denied. Clicking the notification or clicking the button to dismiss the notification causes the notification to be removed from the Notification Center.
  - If the request is approved, a notification is pushed to the Notification Center indicating the request was approved. Behavior for:
    - **application bundles**: Clicking the notification causes the app to be launched and the notification to be removed from the Notification Center.
    - **command-line utilities**: Clicking the notification causes the notification to be removed from the Notification Center. The user will have to manually run the command-line utility from a terminal window. If the user chooses to dismiss the notification, the notification is removed from the Notification Center and no further action is taken.
  - If the approval request fails to be submitted, **Request Approval** is disabled on the Request Approval dialog and an error message displayed.

Deny Execute

This action immediately denies the execution of the application and no interaction with Privilege Manager.app is required. The workflow is:

- macOS will display a dialog indicating the application can't be opened. If the user has granted PrivilegeManager.app the necessary *SendEvents* right, Privilege Manager closes the dialog.
- No further user interaction is provided or necessary.

Deny Execute and Deny Execute Message Action

This action immediately denies the execution of the application. The workflow is:

- macOS will display a dialog indicating the application can't be opened. If the user has granted Privilege Manager.app the necessary *SendEvents* right, Privilege Manager closes the dialog.
- A user notification is posted to the Notification Center that indicates the process was denied.
  - Clicking the notification or clicking the button to dismiss the notification causes the notification to be removed from the Notification Center.
- No further user interaction is necessary.

Deny Execute and Application Denied Message Action

- Privilege Manager immediately denies the execution with macOS displaying a dialog indicating the application can't be opened. If the user has granted Privilege Manager.app the necessary *SendEvents* right, Privilege Manager closes the dialog.
- The custom **Application Denied Message** is shown. **Cancel** and **Publisher Info** are the only buttons enabled.
  - Clicking **Cancel** closes the window.
  - Clicking **Publisher Info** displays certificate information for the application that was denied.
- No further user interaction is necessary.

Application Justification Message Action

This action waits for the user to either **Cancel** or enter a **Justification Message** and click **Continue**. The workflow is:

- Privilege Manager immediately denies the execution with macOS displaying a dialog indicating the application can't be opened. If the user has granted Privilege Manager.app the necessary *SendEvents* right, Privilege Manager closes the dialog.
  - If the user clicks **Cancel**, the dialog is dismissed and no further action taken.
  - If the user clicks **Continue**, the **Justification** will be submitted and the app bundle will be launched.

Application Warning Message Action

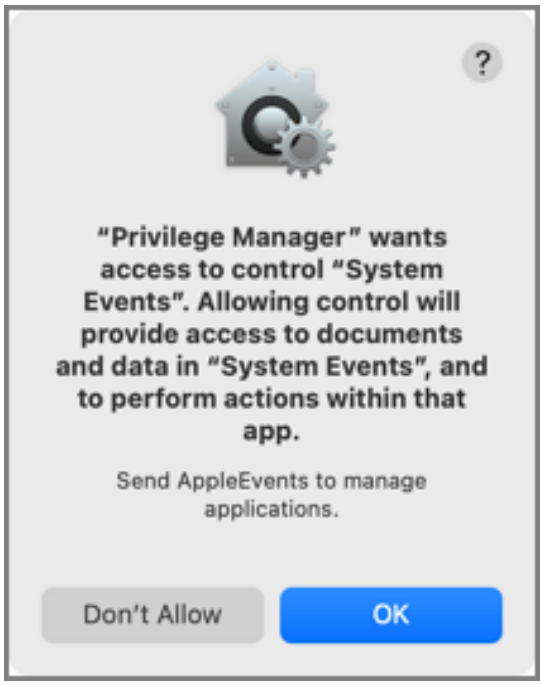
This action waits for the user to either click **Cancel** or **Continue**. The workflow is:

- Privilege Manager immediately denies the execution with macOS displaying a dialog indicating the application can't be opened. If the user has granted Privilege Manager.app the necessary *SendEvents* right, Privilege Manager closes the dialog.
  - If the user clicks **Cancel**, the dialog is dismissed and no further action taken.
  - If the user clicks **Continue**, the app bundle will be launched.

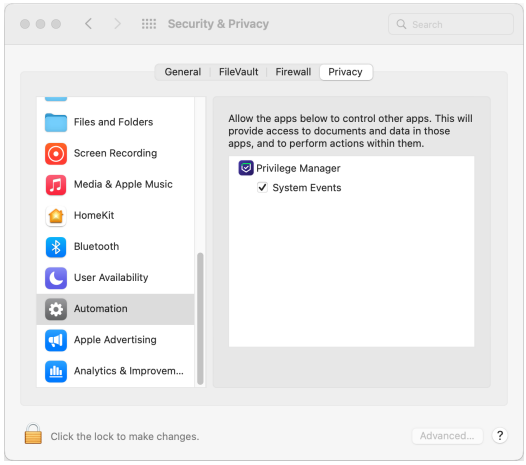
Privacy Preference Policy Control Requests

If you have a policy in Privilege Manager that includes **Deny Execute** or any of the Advanced Message Actions, for example *Application Approval Request*, *Application Denied*, or *Application Justification*, the user at the endpoint might be presented with a macOS dialog saying that the application could not be launched.

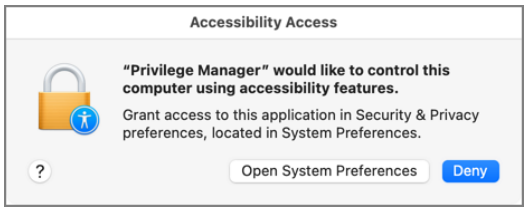
When a policy with one of the above Advanced Message Actions is triggered, Privilege Manager.app attempts to use AppleEvents to dismiss this dialog on behalf of the user to provide the best user experience possible. When Privilege Manager.app attempts to use AppleEvents for the first time, macOS will prompt the user with the following:



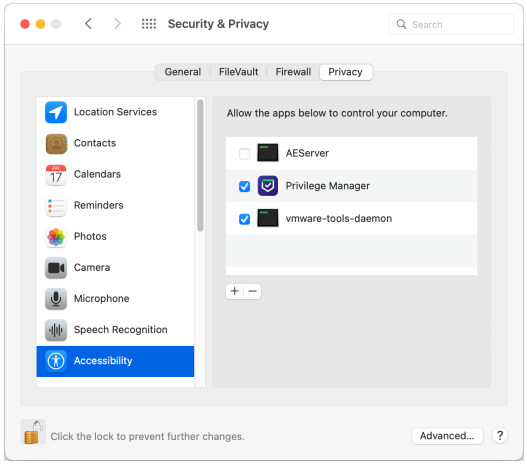
- If the user clicks **OK** on the AppleEvents dialog, System Events will be checked for Privilege Manager.app and it is added to Automation in the Security & Privacy preference pane on the Privacy tab:



- If the user clicks **Don't Allow** on the AppleEvents dialog, the System Events will be unchecked.
- Afterwards, macOS prompts the user with an Accessibility Access dialog:

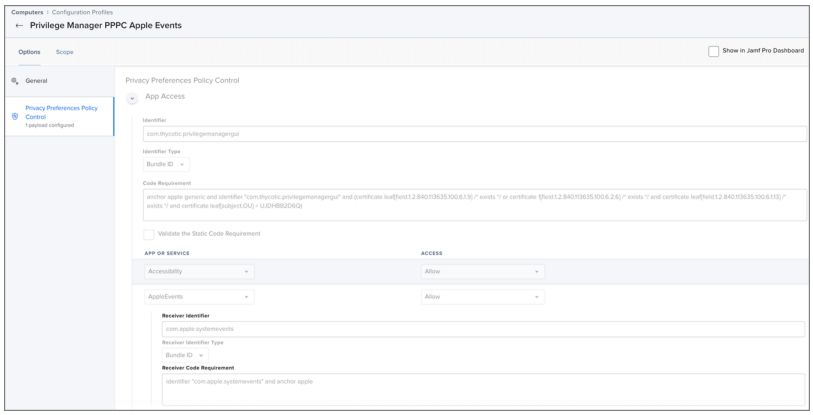


- If the user clicks **Deny**, Privilege Manager.app will not be granted access to use accessibility features to automatically close the dialog that states the application couldn't be launched.
- If the user clicks **Open System Preferences**, the Security & Privacy preference pane opens to the Privacy tab:



If you check **Privilege Manager**, it will be granted access to use accessibility features to control other applications.

In order to automate the approval of these manual prompt(s), use the XML provided here or refer to the Jamf Pro screen shot as an example, depending on your existing MDM.




```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
            <key>PayloadDescription</key>
            <string></string>
            <key>PayloadDisplayName</key>
```

```
            <string>Privacy Preferences Policy Control</string>
            <key>PayloadEnabled</key>
            <true/>
            <key>PayloadIdentifier</key>
            <string>DC4FCA18-FCF2-4332-9192-A00D9A0BC128</string>
            <key>PayloadOrganization</key>
            <string>Thycotic LTD</string>
            <key>PayloadType</key>
            <string>com.apple.TCC.configuration-profile-policy</string>
            <key>PayloadUUID</key>
            <string>DC4FCA18-FCF2-4332-9192-A00D9A0BC128</string>
            <key>PayloadVersion</key>
            <integer>1</integer>
            <key>Services</key>
            <dict>
                <key>Accessibility</key>
                <array>
                    <dict>
                        <key>Allowed</key>
                        <integer>1</integer>
                        <key>CodeRequirement</key>
                        <string>anchor apple generic and identifier
"com.thycotic.privilegemanagergui" and (certificate leaf[field.1.2.840.113635.100.6.1.9]
/* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
UJDHBB2D6Q)</string>
                        <key>Identifier</key>
                        <string>com.thycotic.privilegemanagergui</string>
                        <key>IdentifierType</key>
                        <string>bundleID</string>
                        <key>StaticCode</key>
                        <integer>0</integer>
                    </dict>
                </array>
                <key>AppleEvents</key>
                <array>
                    <dict>
                        <key>AEReceiverCodeRequirement</key>
                        <string>identifier "com.apple.systemevents" and anchor
apple</string>
                        <key>AEReceiverIdentifier</key>
                        <string>com.apple.systemevents</string>
                        <key>AEReceiverIdentifierType</key>
                        <string>bundleID</string>
                        <key>Allowed</key>
                        <integer>1</integer>
                        <key>CodeRequirement</key>
                        <string>anchor apple generic and identifier
"com.thycotic.privilegemanagergui" and (certificate leaf[field.1.2.840.113635.100.6.1.9]
/* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
UJDHBB2D6Q)</string>
                        <key>Identifier</key>
```

```
                        <string>com.thycotic.privilegemanagergui</string>
                        <key>IdentifierType</key>
                        <string>bundleID</string>
                        <key>StaticCode</key>
                        <integer>0</integer>
                    </dict>
                </array>
            </dict>
        </dict>
    </array>
    <key>PayloadDescription</key>
    <string>Privilege Manager PPPC Apple Events</string>
    <key>PayloadDisplayName</key>
    <string>Privilege Manager PPPC Apple Events</string>
    <key>PayloadEnabled</key>
    <true/>
    <key>PayloadIdentifier</key>
    <string>5F761A1C-1F93-4666-99E4-772FDA978AFF</string>
    <key>PayloadOrganization</key>
    <string>Thycotic LTD</string>
    <key>PayloadRemovalDisallowed</key>
    <true/>
    <key>PayloadScope</key>
    <string>System</string>
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadUUID</key>
    <string>5F761A1C-1F93-4666-99E4-772FDA978AFF</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
</dict>
</plist>
```


Block Agent Removal - launchctl

These are the filters and the example policy that need to be created that aid with the macOS agent hardening process.

Creating a File Specification Filter

1. Navigate to **Admin | Filters** and click **Create Filter**.
2. From the platform drop-down select **macOS**.
3. From the type drop-down select **File Specification Filter**.
4. Add a Name and Description, for example */bin/launchctl* and click **Create**.
5. On the filter page, under **Settings**:
   - **File Names**, type `launchctl`.
   - **Path**, type `/bin`.
6. Click **Save Changes**.

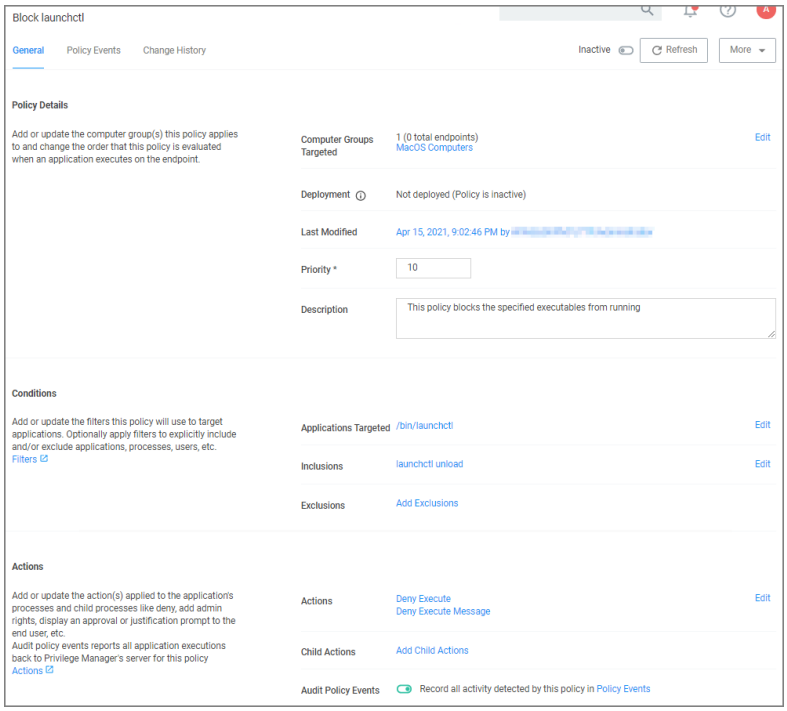
Creating a Commandline Filter

1. Navigate to **Admin | Filters** and click **Create Filter**.
2. From the platform drop-down select **macOS**.
3. From the type drop-down select **Commandline Filter**.
4. Add a Name and Description, for example *launchctl unload* and click **Create**.
5. On the filter page, under **Settings**:
   - **Match Type**, type **Regular Expression**.
   - **Command Line**, type `com\.delinea`.
6. Click **Save Changes**.

Creating the Blocking Policy

1. Under your macOS Computer Group, select **Application Policies**.
2. Using the Policy Wizard, create a controlling policy that blocks application execution on endpoints.
3. Select how you want the processes blocked, either **Block Silently** or **Notify and Block**, for this example we use **Block Silently**. Click **Next Step**.
4. Select what types you want the policy to block, for this example it's **Executables**.
5. Choose your target, for this example **Existing Filter**.
6. Search for and **Add** the **/bin/launchctl** filter created in the above steps.
7. Click **Update**.
8. Click **Next Step**.
9. Name your policy and add a description, click **Create Policy**.
10. Under **Inclusions**, click **Edit**.
11. Search for **launchctl unload** and **Add** the filter created in the above steps.
12. Click **Update**.
13. Click **Save Changes**.

Computer Groups



14. Set the **Inactive** switch to **Active**.

XML Example Files

Policy XML Sample

```
<items>
<CommandlineFilterContract xmlns:adc="http://schemas.arellia.com/dc/"
xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/Arrays"
xmlns:mss="http://schemas.microsoft.com/2003/10/Serialization/"
xmlns:dc="http://schemas.datacontract.org/2004/07/System"
xmlns:d1p4="http://schemas.arellia.com/dc/ClientItem/"
xmlns:i="http://www.w3.org/2001/XMLSchema-
instance" xmlns="http://schemas.arellia.com/dc/ApplicationControl/ApplicationFilter/">
    <adc:FolderId>451680e9-28d1-4af9-8e88-c4cd04f8cebc</adc:FolderId>
    <adc:ItemId>5ab0270c-b9fa-4a8d-b0fe-5dd092971c92</adc:ItemId>
    <adc:Name>launchctl unload</adc:Name>
    <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
    <adc:Strings />
    <adc:Tags>
        <arr:string>pm.platform.macos</arr:string>
    </adc:Tags>
    <Commandline>com.\thycotic</Commandline>
    <Option>2</Option>
</CommandlineFilterContract>
```

```
<FileSpecificationFilterContract xmlns:adc="http://schemas.arellia.com/dc/"
xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/Arrays"
xmlns:mss="http://schemas.microsoft.com/2003/10/Serialization/"
xmlns:dc="http://schemas.datacontract.org/2004/07/System"
xmlns:d1p4="http://schemas.arellia.com/dc/ClientItem/"
xmlns:i="http://www.w3.org/2001/XMLSchema-
instance" xmlns="http://schemas.arellia.com/dc/FileInventory/Filters/">
    <adc:FolderId>451680e9-28d1-4af9-8e88-c4cd04f8cebc</adc:FolderId>
    <adc:ItemId>ebbd1adf-72f6-4e71-bbb0-46417ecdbd8b</adc:ItemId>
    <adc:Name>/bin/launchctl</adc:Name>
    <adc:ProductId>75afc25f-c518-491c-a60d-ecd6b7dbc7ad</adc:ProductId>
    <adc:Strings />
    <adc:Tags>
        <arr:string>pm.platform.macos</arr:string>
    </adc:Tags>
    <ChildAssociations>
        <arr:anyType i:type="adc:ItemAssociations">
            <adc:AssociationTypeId>efb89861-0aed-5592-be87-
6c8992773a87</adc:AssociationTypeId>
            <adc:AssociatedItemIds />
        </arr:anyType>
        <arr:anyType i:type="adc:ItemAssociations">
            <adc:AssociationTypeId>c01776a1-dffd-5842-94ad-
aedbafc19515</adc:AssociationTypeId>
            <adc:AssociatedItemIds />
        </arr:anyType>
    </ChildAssociations>
    <DriveTypes>0</DriveTypes>
    <ExcludeFilterIds />
    <FilePath>/bin/</FilePath>
    <FileSpec>launchctl</FileSpec>
    <IncludeFilterIds />
    <IncludeHidden>false</IncludeHidden>
    <IncludeReparse>true</IncludeReparse>
    <IncludeSubdirectories>false</IncludeSubdirectories>
    <IncludeSystem>false</IncludeSystem>
    <IncludeSystemReparse>false</IncludeSystemReparse>
    <ManditoryFilterIds />
    <OwnsItemIds />
</FileSpecificationFilterContract>
<ApplicationControlPolicyContract xmlns:adc="http://schemas.arellia.com/dc/"
xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/Arrays"
xmlns:mss="http://schemas.microsoft.com/2003/10/Serialization/"
xmlns:dc="http://schemas.datacontract.org/2004/07/System"
xmlns:i="http://www.w3.org/2001/XMLSchema-
instance" xmlns="http://schemas.arellia.com/dc/ApplicationControl/Policy/">
    <adc:Description>This policy blocks the specified executables from
running</adc:Description>
    <adc:FolderId>74cbc043-beed-499f-85ca-cc10d1bf44d5</adc:FolderId>
    <adc:ItemId>187b30cb-803c-4ba2-a8ab-39ebf905716b</adc:ItemId>
    <adc:Name>Block launchctl</adc:Name>
    <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
    <adc:Strings />
```

```
    <adc:Tags>
        <arr:string>pm.platform.macos</arr:string>
        <arr:string>pm.policyType:block</arr:string>
    </adc:Tags>
    <adc:ApplyToResourcesSettings xmlns:d2p1="http://schemas.arellia.com/dc/Resource/">
        <d2p1:AllowedTargetRoleTypeId>493435f7-3b17-4c4c-b07f-
c23e7ab7781f</d2p1:AllowedTargetRoleTypeId>
        <d2p1:RequiresScopingSecurity>false</d2p1:RequiresScopingSecurity>
        <d2p1:RestrictionCollectionId>00000000-0000-0000-0000-
000000000000</d2p1:RestrictionCollectionId>
        <d2p1:ScopingSecurityOperationId>00000000-0000-0000-0000-
000000000000</d2p1:ScopingSecurityOperationId>
    </adc:ApplyToResourcesSettings>
    <adc:DefaultResourceTargetIds>
        <arr:guid>34166591-d5f2-4dde-abc3-99d5aa841518</arr:guid>
    </adc:DefaultResourceTargetIds>
    <adc:Enabled>false</adc:Enabled>
    <ApplicationActionIds>
        <arr:guid>d8498d12-4fdd-44db-b21c-4e294881c4d4</arr:guid>
        <arr:guid>01b913fe-b098-4ec9-99fe-ec93782da543</arr:guid>
    </ApplicationActionIds>
    <AppliesToAllProcesses>false</AppliesToAllProcesses>
    <ChildApplicationActionIds />
    <ChildAssociations />
    <EndsProcessing>true</EndsProcessing>
    <EndsProcessingChild>false</EndsProcessingChild>
    <ManditoryFilterIds>
        <arr:guid>5ab0270c-b9fa-4a8d-b0fe-5dd092971c92</arr:guid>
    </ManditoryFilterIds>
    <NegativeFileFilterIds />
    <OwnsItemIds />
    <PositiveFileFilterIds>
        <arr:guid>ebbd1adf-72f6-4e71-bbb0-46417ecdbd8b</arr:guid>
    </PositiveFileFilterIds>
    <Priority>10</Priority>
    <SendActionEvent>true</SendActionEvent>
    <SkipDuringSystemStartup>false</SkipDuringSystemStartup>
    <Stage2Processing>false</Stage2Processing>
</ApplicationControlPolicyContract>

</items>
```


File Specification Filter


```
<items>
<FileSpecificationFilterContract xmlns:adc="http://schemas.arellia.com/dc/"
xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/Arrays"
xmlns:mss="http://schemas.microsoft.com/2003/10/Serialization/"
xmlns:dc="http://schemas.datacontract.org/2004/07/System"
xmlns:d1p4="http://schemas.arellia.com/dc/ClientItem/"
xmlns:i="http://www.w3.org/2001/XMLSchema-
instance" xmlns="http://schemas.arellia.com/dc/FileInventory/Filters/">
    <adc:FolderId>451680e9-28d1-4af9-8e88-c4cd04f8cebc</adc:FolderId>
```

```
    <adc:ItemId>ebbd1adf-72f6-4e71-bbb0-46417ecdbd8b</adc:ItemId>
    <adc:Name>/bin/launchctl</adc:Name>
    <adc:ProductId>75afc25f-c518-491c-a60d-ecd6b7dbc7ad</adc:ProductId>
    <adc:Strings />
    <adc:Tags>
        <arr:string>pm.platform.macos</arr:string>
    </adc:Tags>
    <ChildAssociations>
        <arr:anyType i:type="adc:ItemAssociations">
            <adc:AssociationTypeId>efb89861-0aed-5592-be87-
6c8992773a87</adc:AssociationTypeId>
            <adc:AssociatedItemIds />
        </arr:anyType>
        <arr:anyType i:type="adc:ItemAssociations">
            <adc:AssociationTypeId>c01776a1-dffd-5842-94ad-
aedbafc19515</adc:AssociationTypeId>
            <adc:AssociatedItemIds />
        </arr:anyType>
    </ChildAssociations>
    <DriveTypes>0</DriveTypes>
    <ExcludeFilterIds />
    <FilePath>/bin/</FilePath>
    <FileSpec>launchctl</FileSpec>
    <IncludeFilterIds />
    <IncludeHidden>false</IncludeHidden>
    <IncludeReparse>true</IncludeReparse>
    <IncludeSubdirectories>false</IncludeSubdirectories>
    <IncludeSystem>false</IncludeSystem>
    <IncludeSystemReparse>false</IncludeSystemReparse>
    <ManditoryFilterIds />
    <OwnsItemIds />
</FileSpecificationFilterContract>

</items>
```


Commandline Filter

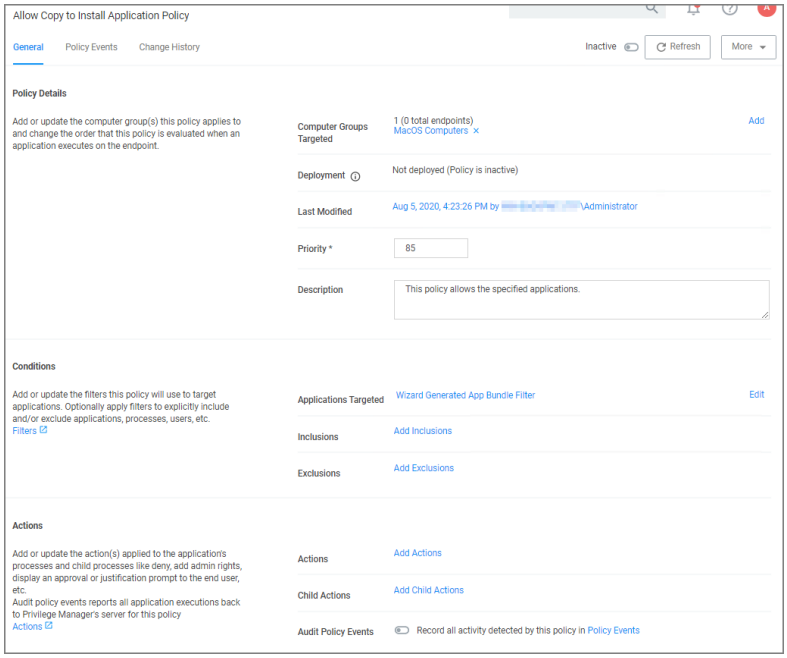

```
<items>
<CommandlineFilterContract xmlns:adc="http://schemas.arellia.com/dc/"
xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/Arrays"
xmlns:mss="http://schemas.microsoft.com/2003/10/Serialization/"
xmlns:dc="http://schemas.datacontract.org/2004/07/System"
xmlns:d1p4="http://schemas.arellia.com/dc/ClientItem/"
xmlns:i="http://www.w3.org/2001/XMLSchema-
instance" xmlns="http://schemas.arellia.com/dc/ApplicationControl/ApplicationFilter/">
    <adc:FolderId>451680e9-28d1-4af9-8e88-c4cd04f8cebc</adc:FolderId>
    <adc:ItemId>5ab0270c-b9fa-4a8d-b0fe-5dd092971c92</adc:ItemId>
    <adc:Name>launchctl unload</adc:Name>
    <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
    <adc:Strings />
    <adc:Tags>
        <arr:string>pm.platform.macos</arr:string>
    </adc:Tags>
```

```
    <Commandline>com.\thycotic</Commandline>
    <Option>2</Option>
</CommandlineFilterContract>

</items>
```

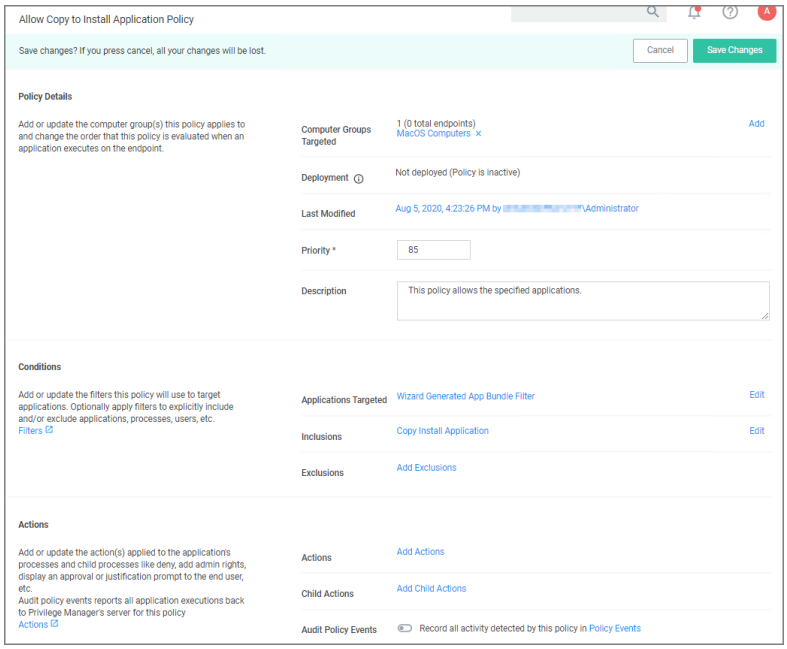
Allow Copy to Install Applications

A policy can be created to allow or deny standard users to install specific applications by dragging-and-dropping the application into the /Applications folder. Follow this example to create a policy that will enable this functionality for macOS standard users. This example policy has been verified for use with KEXT and SYSEX agent workstations.

1. Navigate to your macOS Computer Group and select **Application Policies**.
2. Click **Create Policy**.
3. Select **Controlling** and click **Next Step**.
4. Select **Allow** and click **Next Step**.
5. Select what exactly you want the policy to target. This can be based of an **Existing Filter**, a **File Upload**, and/or **Inventoried File(s)**. Multiple targets can be selected.
6. Click **Next Step**.
7. Enter a Name and description for your policy, click **Create Policy**.



8. Click **Add Inclusions**.
9. Search for and add the **Copy Install Application** filter.
10. Click **Update**.



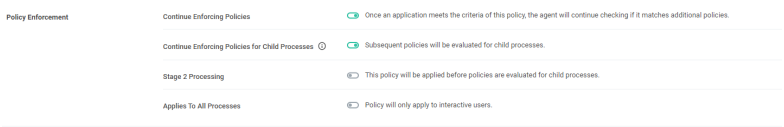
11. Click **Save Changes**.
12. Set the **Inactive** switch to **Active** for policy updates at the endpoint.

> **Note:** The new Copy Install Application Filter should not be used with the existing Privilege Manager Copy/Installer Helper Parent Process Filter, which should be removed from any policy before adding the new Copy Install Application Filter to the policy.

Updating Existing Policies to Use the Copy Install Application Filter

If you have policies that currently use the Privilege ManagerCopy/Installer Helper Parent Process Filter use the following steps to update them to use the Copy Install Application Filter in the Privilege Manager UI:

1. Navigate to the macOS Computers Group and select **Application Policies**.
2. For each application that currently uses the **Privilege manager copy/installer helper parent process filter** as an inclusion filter, remove that filter and add the **Copy Install Application** filter instead.
3. Click **Update**.
4. Under Actions remove **Allow copy to /Applications Directory** and add the **Application Approval Request Message Action** in its place.
5. Click **Update**.
6. Click **Show Advanced** and set these two option to active:
   - Continue Enforcing.
   - Enforce Child Processes.

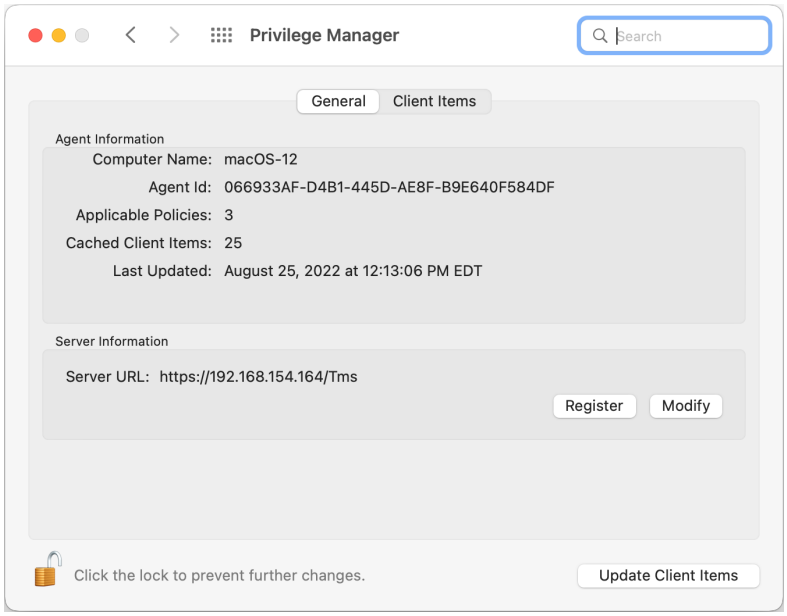


7. Click **Save Changes**.

Updating the Workstation

On the macOS workstation:

1. Open **System Preferences | Privilege Manager**.

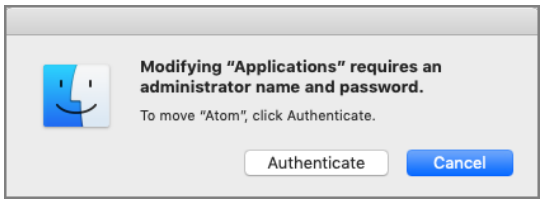


2. Click **Update Client Items**.

The agent updates with new and updated policies and synchronizes.

Expected User Experience

After the policies are updated, users can open a DMG or just drag-and-drop an application bundle to /Applications. Depending on the version of macOS, users may see a dialog asking to authenticate by clicking **Authenticate**. Users will not be prompted for admin credentials to complete the operation.



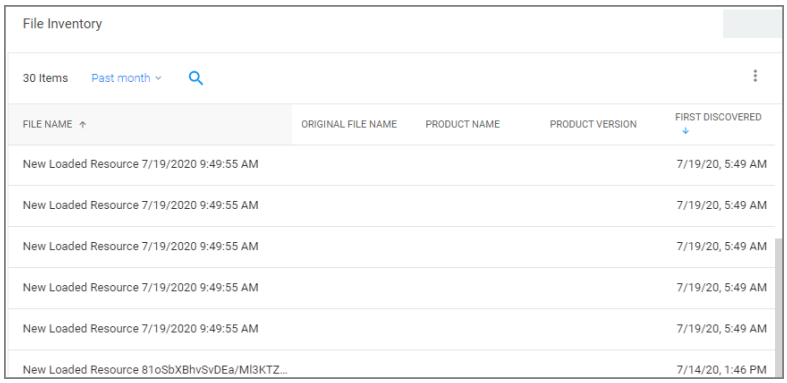
Deny Zoom Application

With your monitoring policies properly set up, anything you do on your Mac test machine will be discovered by Privilege Manager. For this example we will create a policy that blocks the Zoom application.

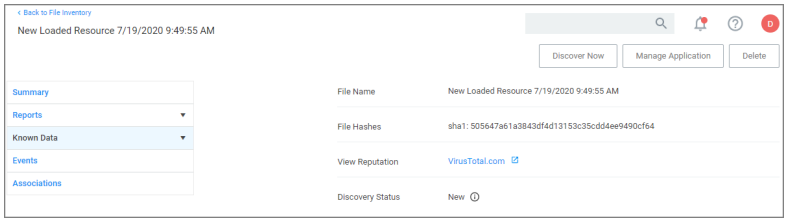
File Inventory

Open the Zoom application on a macOS test workstation. When the application is opened, Privilege Manager discovers it as an *Application Action from Event Discovery Testing Computers Audit Policy (macOS)*.

1. In the Privilege ManagerConsole, navigate to **File Inventory**.
2. Verify new items have been registered by your Event Discovery Testing Computers (macOS) policy. These may be listed as **New Loaded Resources**.



3. Select a **New Loaded Resource** link.
4. On the loaded Resource Explorer page, click **Discover Now**. It still may take time to properly load details about these new events, usually indicated by a **Discovery Status** of **New**.

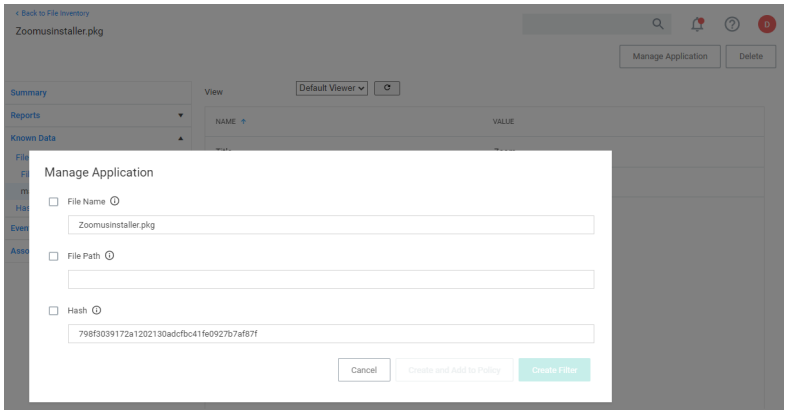


Clicking **Discover Now** creates and executes a **Manual client-side resource discovery** task. If you click the status link the task page opens (not shown in this example sequence).

On the Resource Explorer page of a fully discovered resource, you can click **Manage Application** to select the option you want to use, which is to either

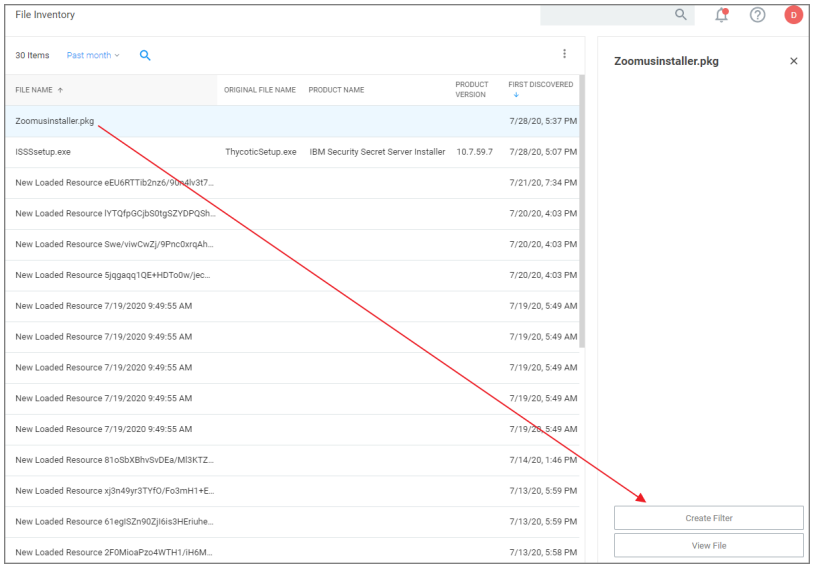
- create a filter, or

- create and add to a policy.



When a resource is fully discovered it is displayed with full name on the discovery events page:

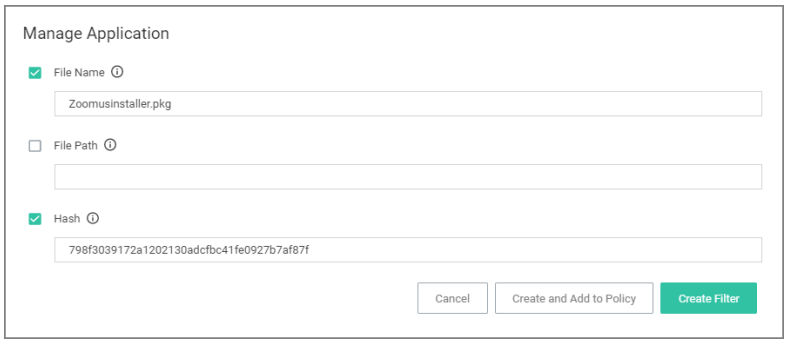
From the File Inventory page you can also use the **View File** or **Create Filter** options to create specific filters for the discovered applications and assign those to existing policies.



Assign to Policy

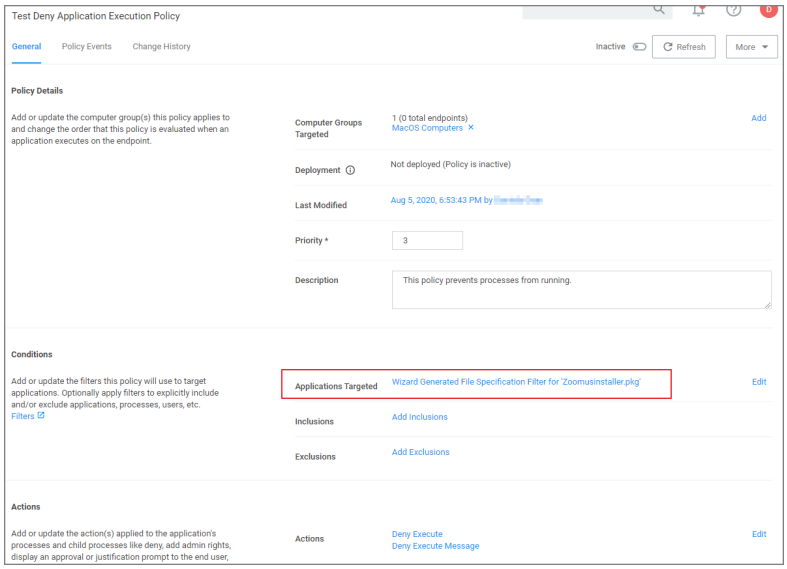
Once the resources have been fully discovered, the fastest way to either create a new policy or add to an existing one is via the Assign to Policy link on the Events page.

1. Click **Create Filter**.
2. The **Manage Application** page opens for the selected resource.



3. Click **Create and Add To Policy**.

4. On the **Manage Application** page select your existing deny application execution policy from the drop-down and click **Update Policy**.

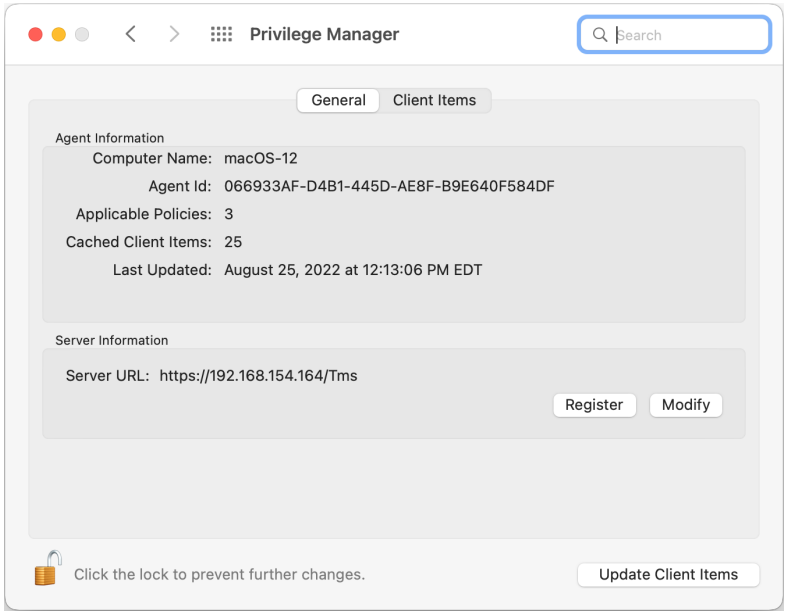


5. Set the **Inactive** switch to **Active**.

Updating the Workstation

On the macOS workstation:

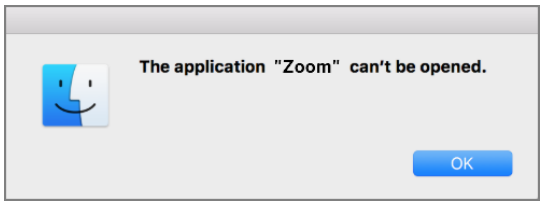
1. Open **System Preferences | Privilege Manager**.



2. Click **Update Client Items**.

Policy Verification

Once this Deny policy is updated on your workstation, when you click Zoom, you will see a message like this:



Elevating Activity Monitor

Authorizationdb Right: com.apple.activitymonitor.kill

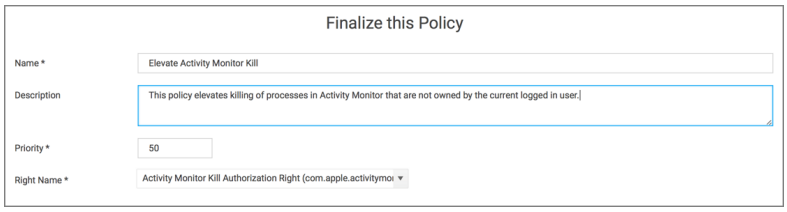
This action can be used to elevate killing processes that do not belong to the logged in user in Activity Monitor while it is running. The right will be elevated for the duration that Activity Monitor is running. Once the application is quit, the right will be restored to its default.

Advanced message actions such as Approval, Deny, Justification, or Warning should not be used in conjunction with this action.

Example Application: Activity Monitor

1. Using the Policy Wizard, create a controlling policy, click **Next Step**.
2. Select **Elevate**, click **Next Step**.

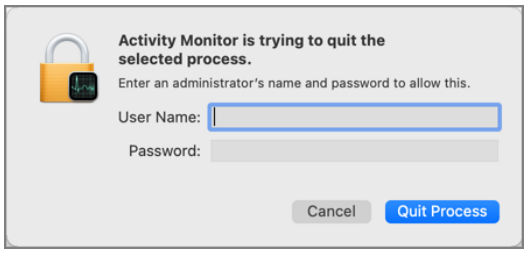
3. Select **Run Silently**, click **Next Step**.
4. Select **Executables**, click **Next Step**.
5. Select **Modify Authorization Database**, click **Next Step**.
6. Select **Existing Filter**, search for select the App Bundle filter for Activity Monitor. If it doesn't exist, create it.
7. Click **Update**.
8. Click **Next Step**.
9. Name your policy, add a description.
10. From the **Right Name** drop-down, select **Activity Monitor Kill Authorization Right (com.apple.activitymonitor.kill)**.



11. Click **Create Policy**.
12. Set the **Inactive** switch to **Active**.
13. Next to **Deployment** click the **i** icon and run the **Resource and Collection Targeting Update** task.

What to Expect on the Endpoint

- **With** a policy in place, when Activity Monitor is running and the policy is effective and you try to kill a process that doesn't belong to you and you click **Force Quit**, the process will be terminated without prompting you for admin credentials.
- **Without** a policy in place, when Activity Monitor is running and you try to kill a process that doesn't belong to you, it will present this dialog:



Elevating Charles Proxy

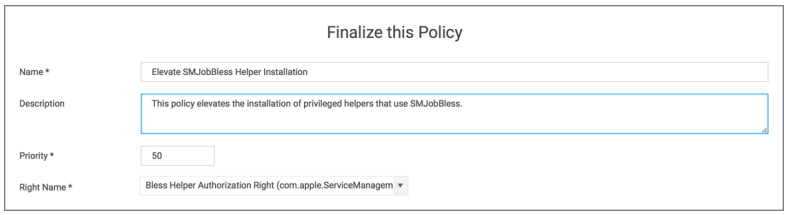
Authorizationdb Right: com.apple.ServiceManagement.blesshelper

This action deals with applications that use SMJobBless to install privileged helpers. This action can be used to elevate the installation of a privileged helper while an application is running. The right will be elevated for the duration of the targeted application. Once the application is quit, the right will be restored to its default.

Advanced message actions such as Approval, Deny, Justification, or Warning should not be used in conjunction with this action.

Example Application: Charles Proxy

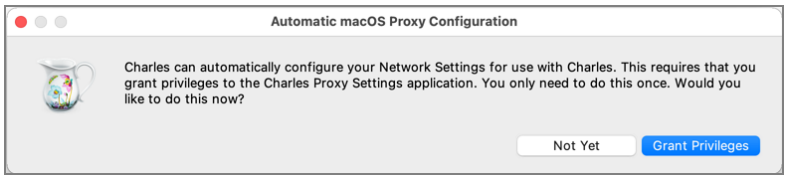
1. Using the Policy Wizard, create a controlling policy, click **Next Step**.
2. Select **Elevate**, click **Next Step**.
3. Select **Run Silently**, click **Next Step**.
4. Select **Executables**, click **Next Step**.
5. Select **Modify Authorization Database**, click **Next Step**.
6. Select **Existing Filter**, search for select the App Bundle filter for Charles Proxy. If it doesn't exist, create it.
7. Click **Update**.
8. Click **Next Step**.
9. Name your policy, add a description.
10. From the **Right Name** drop-down, select **Bless Helper Authorization Right (com.apple.ServiceManagement.blesshelper)**.



11. Click **Create Policy**.
12. Set the **Inactive** switch to **Active**.
13. Next to **Deployment** click the **i** icon and run the **Resource and Collection Targeting Update** task.

What to Expect on the Endpoint

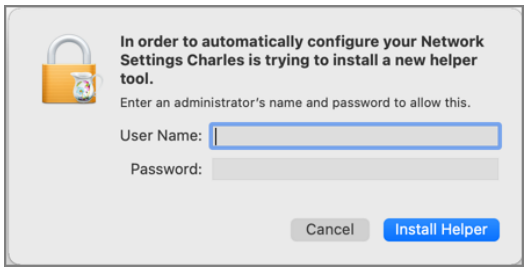
- **With** a policy in place, when Charles Proxy is started and the policy is effective and its helper isn't installed, it will present this dialog:



  Clicking **Grant Privileges** will approve the installation of the helper without prompting for admin credentials.

- **Without** a policy in place, when Charles Proxy is started and its helper isn't installed, it will present an

authorization required dialog:



Note: Privileges to the Helper, if not already installed, need to be granted no matter if a policy is in place or not. Granting those privileges, however won't require an authorization when a policy with Bless Helper Authorization Right action is in place and active.

How to Allow a Standard User to Upgrade to macOS Big Sur

Refer to the example video for details.

Elevating Modifying the Keychain

Authorizationdb Right: system.keychain.modify

This action can be used to elevate modifying the System keychain in Keychain Access while it is running. The right will be elevated for the duration that Keychain Access is running. Once the application is quit, the right will be restored to its default.

Advanced message actions such as Approval, Deny, Justification, or Warning should not be used in conjunction with this action.

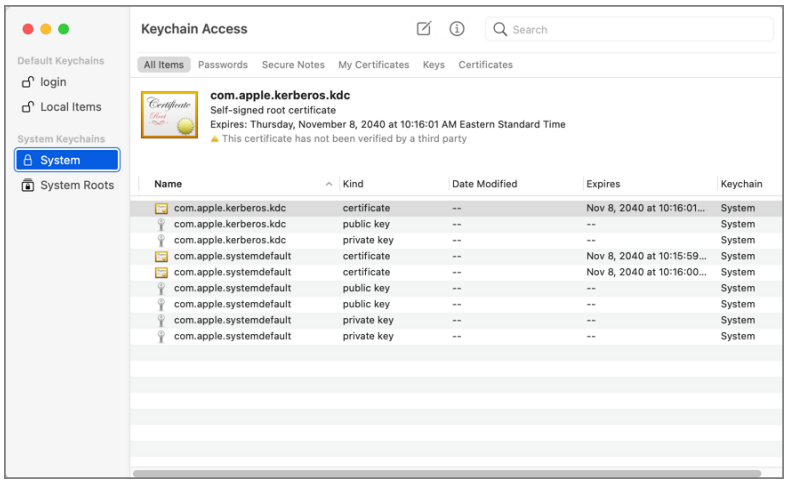
Example Application: Keychain Access

1. Using the Policy Wizard, create a controlling policy, click **Next Step**.
2. Select **Elevate**, click **Next Step**.
3. Select **Run Silently**, click **Next Step**.
4. Select **Executables**, click **Next Step**.
5. Select **Modify Authorization Database**, click **Next Step**.
6. Select **Existing Filter**, search for and select the App Bundle filter for Keychain Access. If it doesn't exist, create it.
7. Click **Update**.
8. Click **Next Step**.
9. Name your policy, add a description.
10. From the **Right Name** drop-down, select **Modify System Keychain Authorization Right (system.keychain.modify)**.

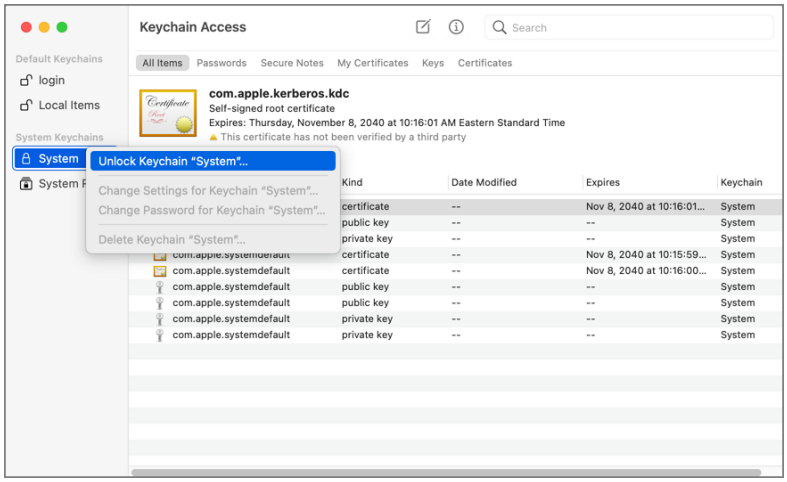
11. Click **Create Policy**.
12. Set the **Inactive** switch to **Active**.
13. Next to **Deployment** click the **i** icon and run the **Resource and Collection Targeting Update** task.

What to Expect on the Endpoint

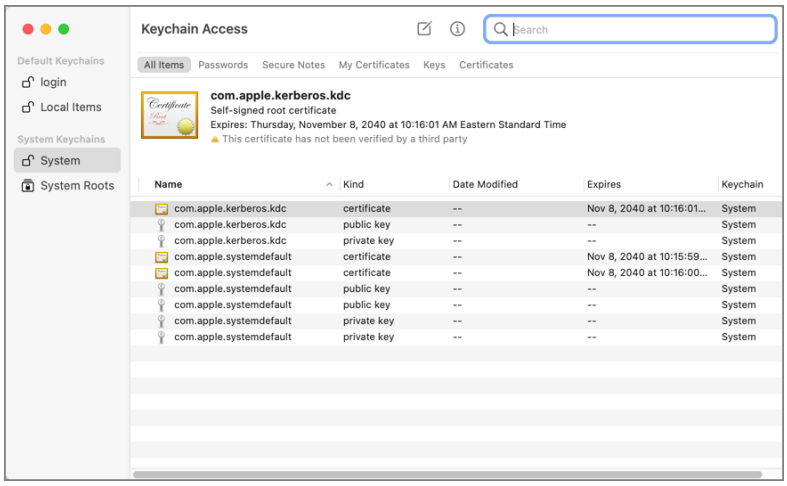
- **With** a policy in place, with Keychain Access running and the policy is effective, the System keychain icon will appear to be locked:



When you right-click the System keychain icon, the Unlock Keychain "System" menu item will appear:



When you click on Unlock Keychain "System", the System keychain will be unlocked and you can add and delete items without being prompted for admin credentials:



- **Without** a policy in place, when Keychain Access is running and you try to unlock or modify the System keychain, it will present this dialog:

Elevating Xcode

Xcode relies on two authorizationdb rights to provide certain aspects of its functionality:

- The acknowledgment of the license agreement upon first run after being installed.
- The ability to install iOS simulators.

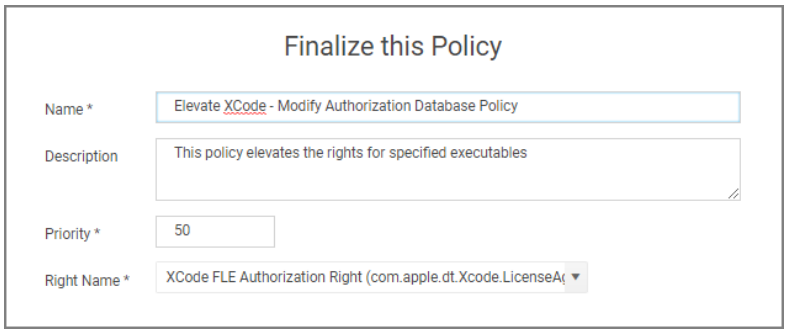
Agree to License Agreement

The default right to agree to the license agreement Xcode uses, requires the user to be in the admin's group and will prompt for admin credentials.

To elevate this aspect of Xcode, you can create a policy that targets Xcode and has the Xcode FLE Authorization Right (com.apple.dt.Xcode.LicenseAgreementXPCServiceRights) Authorization DB Right Name.

Advanced message actions such as Approval, Deny, Justification, or Warning should not be used in conjunction with this action.

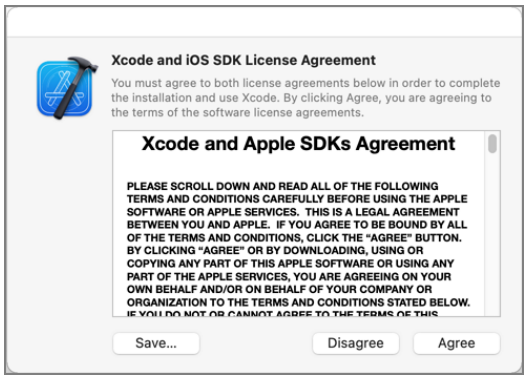
1. Using the Policy Wizard, create a controlling policy, click **Next Step**.
2. Select **Elevate**, click **Next Step**.
3. Select **Run Silently**, click **Next Step**.
4. Select **Executables**, click **Next Step**.
5. Select **Modify Authorization Database**, click **Next Step**.
6. Select **Existing Filter**, search for and use an App Bundle filter that targets Xcode. If one doesn't exist, create it.
7. Click **Update**.
8. Click **Next Step**.
9. Name your policy, add a description.
10. From the **Right Name** drop-down, select **Xcode FLE Authorization Right (com.apple.dt.Xcode.LicenseAgreementXPCServiceRights)**.



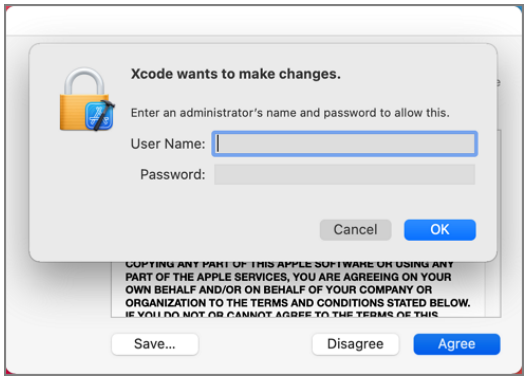
11. Click **Create Policy**.
12. Set the **Inactive** switch to **Active**.
13. Next to **Deployment** click the **i** icon and run the **Resource and Collection Targeting Update** task.

What to Expect on the Endpoint

- **With** a policy in place, when Xcode is run the first time and the user is a standard user and the policy is effective, the user will only be prompted to agree to the license agreement:



- **Without** policy in place, when Xcode is run the first time and the user is a standard user, it prompts to agree to the license agreement. Clicking Agree results in the user being asked to provide admin credentials:



Install iOS Simulators

Xcode uses a right that requires the user to be in the admin's group to install iOS Simulators. By default, when a standard user tries to install an iOS simulator they will be prompted to enter admin credentials.

To elevate this aspect of Xcode, you can create a policy that targets Xcode and has the Install Apple Software Authorization Right (system.install.apple-software) Authorization DB Right Name.

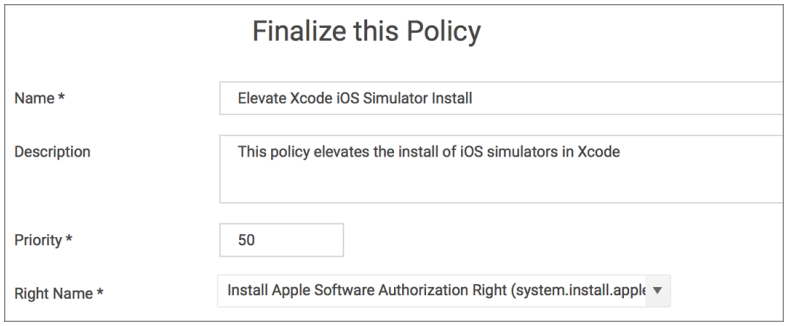
You can add this to a policy that already targets Xcode to elevate the license agreement with the XCode FLE Authorization Right (com.apple.dt.Xcode.LicenseAgreementXPCServiceRights) Authorization DB Right Name or you can create a policy that targets Xcode and this Authorization DB Right Name specifically.

To elevate this aspect of Xcode specifically, you can create a policy that targets Xcode and has the Install Apple Software Authorization Right (system.install.apple-software) Authorization DB Right Name.

Advanced message actions such as Approval, Deny, Justification, or Warning should not be used in conjunction with this action.

1. Using the Policy Wizard, create a controlling policy, click **Next Step**.
2. Select **Elevate**, click **Next Step**.
3. Select **Run Silently**, click **Next Step**.
4. Select **Executables**, click **Next Step**.

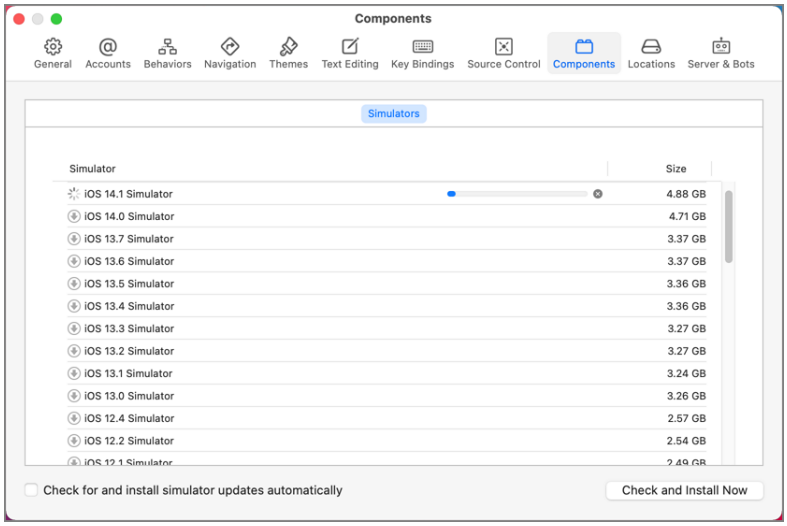
5. Select **Modify Authorization Database**, click **Next Step**.
6. Select **Existing Filter**, search for and use an App Bundle filter that targets Xcode. If one doesn't exist, create it.
7. Click **Update**.
8. Click **Next Step**.
9. Name your policy, add a description.
10. From the **Right Name** drop-down, select **Install Apple Software Authorization Right (system.install.apple-software)**.



11. Click **Create Policy**.
12. Set the **Inactive** switch to **Active**.
13. Next to **Deployment** click the **i** icon and run the **Resource and Collection Targeting Update** task.

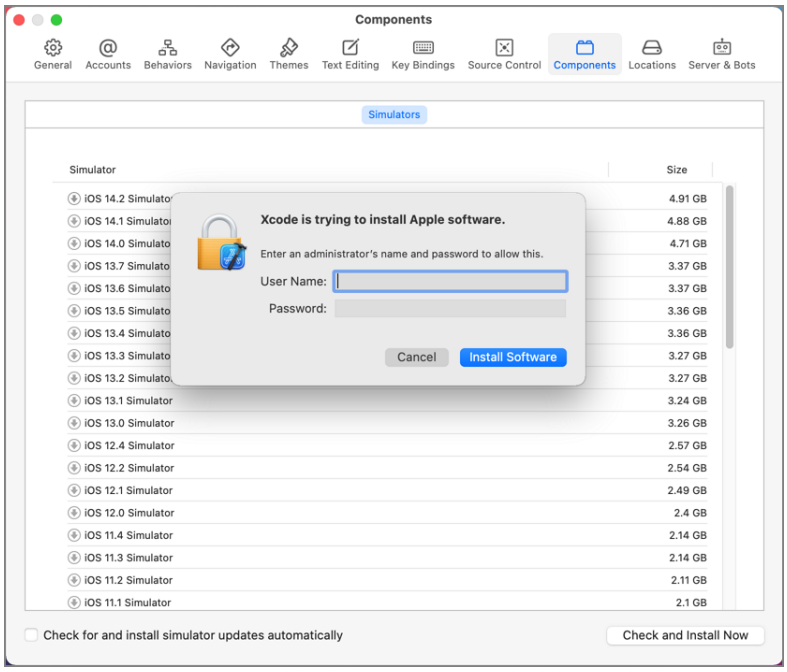
What to Expect on the Worksation

- **With** a policy in place, when a standard user attempts to install an iOS simulator and the policy is effective, the install will begin without prompting for credentials:



- **Without** a policy in place, by default, when a standard user attempts to install an iOS simulator they will be

prompted for admin credentials:



Enabling Developer Mode

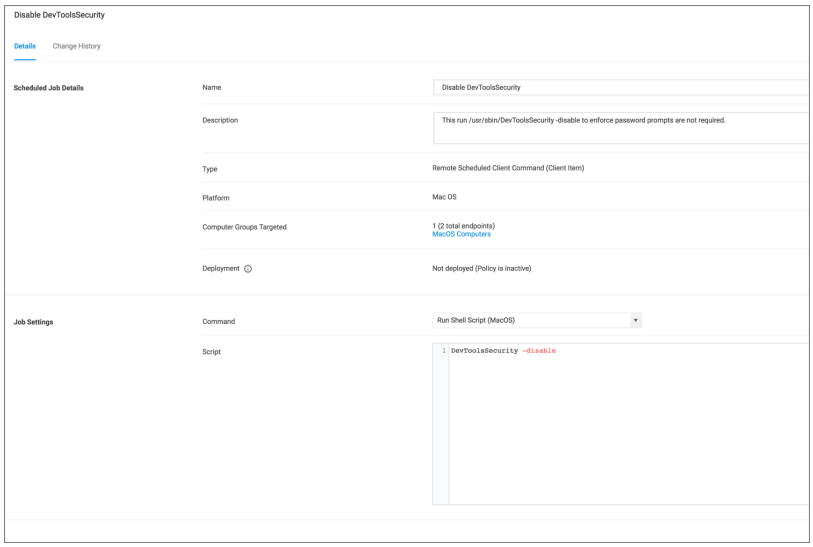
By default, Xcode's Developer mode is disabled. When disabled, Xcode will prompt for admin credentials when the debugger or performance analysis tools are used to examine a process. If the user is a member of the **_developer** group, the user will be prompted for their credentials instead.

The man page for DevToolsSecurity says:

"This tool changes the security authorization policies for use of Apple-code-signed debugger and performance analysis tools on development systems.

On normal user systems, the first time in a given login session that any such Apple-code-signed debugger or performance analysis tools are used to examine one of the user's processes, the user is queried for an administrator password for authorization. Use the DevToolsSecurity tool to change the authorization policies, such that a user who is a member of either the admin group or the **_developer** group does not need to enter an additional password to use the Apple-code-signed debugger or performance analysis tools." (macOS system man page quote)

Depending on your requirements, you can address the issue of the user being prompted for admin credentials by adding your users to the **_developer** group via LSS. If you wish to enable Developer mode and avoid the dialog entirely, you can create a scheduled command (client task) in Privilege Manager to run the DevToolsSecurity command and enforce it on specific workstations based on the LSS group membership.



macOS Homebrew Installer Support

If you are using Homebrew to manage command line utilities and applications, you need to add the user to the admin group with a JIT group action and use a policy with additional advanced settings as described below.

With a policy in place, a standard (non-admin) user is able to run the Homebrew installer by entering the command line found on the Homebrew home page (https://brew.sh) at a Terminal window prompt. After that the installer proceeds and completes successfully, resulting in a Homebrew installation under `/usr/local` (or `/opt/homebrew` on Apple Silicon machines) owned by the user (not root).

Refer to this video demonstration.

Note: Not supported on endpoints running the KEXT agent.

Copying any example text below and pasting it into filters, actions, or policies being set up on a server, might introduce special characters in pasted text, which can cause policies to fail.

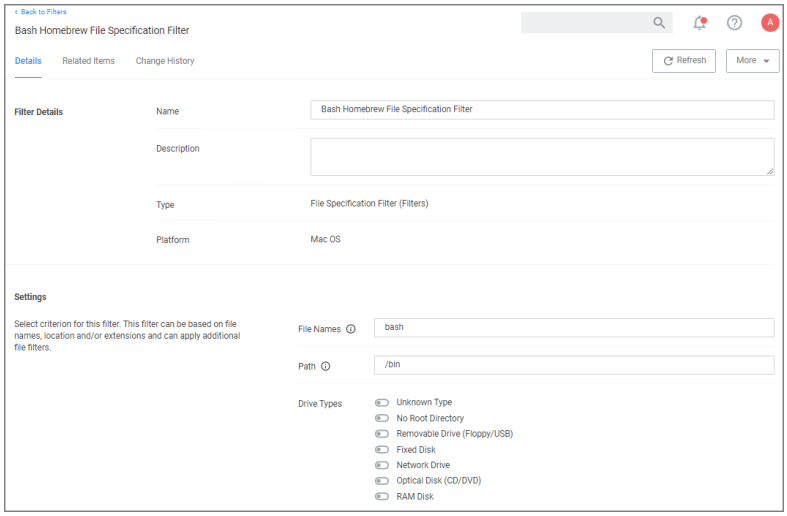
Creating the Filters Needed

Create a Bash File Specification Filter

This filter will specify the applications targeted.

1. Navigate to **Admin | Filters**.
2. Click **Create Filter**.
3. From the **Platform** drop-down, select **macOS**.
4. From the **Type** drop-down, select **File Specification Filter**.
5. Name the filter and provide a description to reflect the purpose, for example **Bash Homebrew File Specification Filter**.
6. Click **Create**.

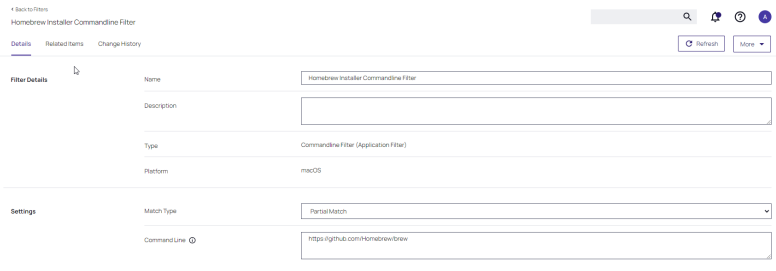
7. Under **Settings | File Names**, enter **bash**.
8. For **Path**, enter **/bin**.
9. Click **Save Changes**.



Create a Homebrew Installer Commandline Filter

This filter will be added as an inclusion filter.

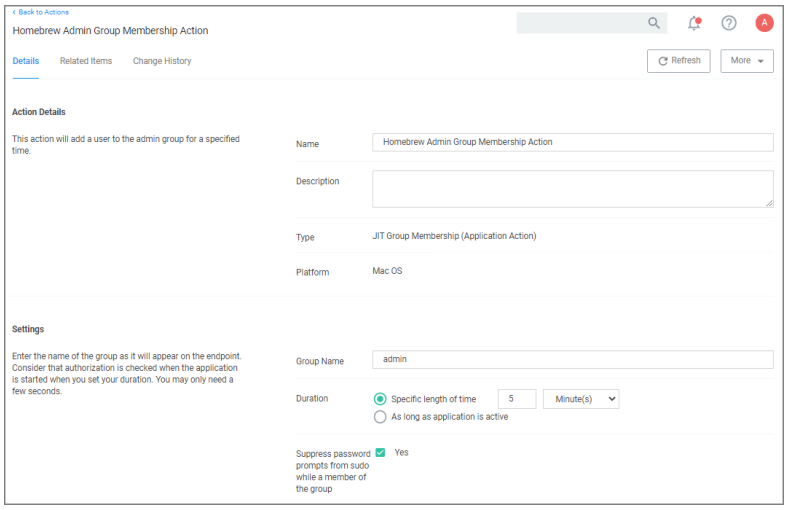
1. Navigate to **Admin | Filters**.
2. Click **Create Filter**.
3. From the **Platform** drop-down, select **macOS**.
4. From the **Type** drop-down, select **Commandline Filter**.
5. Name the filter and provide a description to reflect the purpose, for example **Homebrew Installer Commandline Filter**.
6. Click **Create**.
7. Under **Settings | Match Type**, select **Partial Match**.
8. For **Command Line**, enter `https://github.com/Homebrew/brew`.
9. Click **Save Changes**.



Creating the Homebrew Admin Group Membership Action

This action will be added under Actions section of the policy.

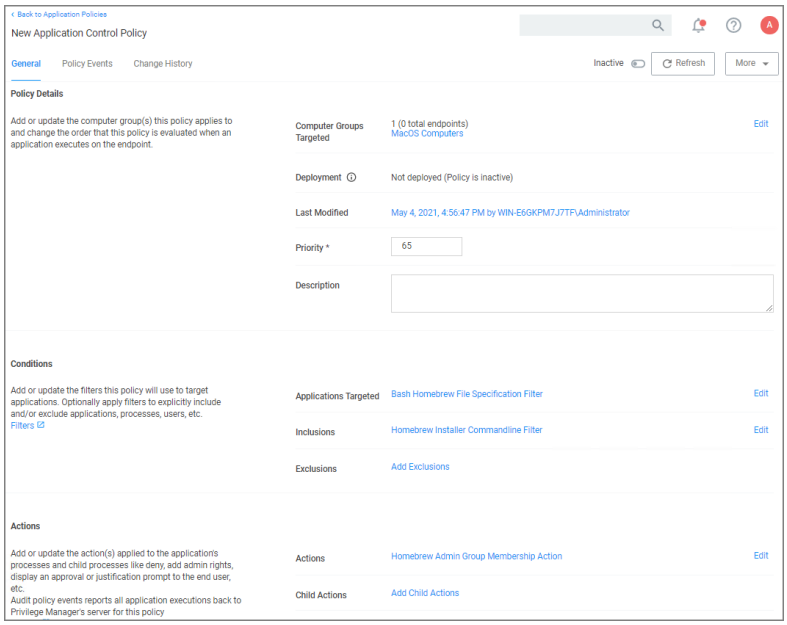
1. Navigate to **Admin | Actions**.
2. Click **Create Action**.
3. From the **Platform** drop-down, select **macOS**.
4. From the **Type** drop-down, select **Just-in-Time Group Membership Action**.
5. Name the Action and provide a description to reflect the purpose, for example **Homebrew Admin Group Membership Action**.
6. Click **Create**.
7. Under **Settings | Group Name**, enter **admin**.
8. For **Duration** keep the default 5 min setting.
9. For **Suppress password prompts from sudo while a member of the group** set the checkmark to change to yes.
10. Click **Save Changes**.



Creating the Homebrew Installation Policy

1. Navigate to your macOS computer group and select **Application Policies**.
2. Click **Create Policies**.
3. Select **Skip the wizard, take me to a blank policy** option.
4. Name the policy, for example **Homebrew Installation Policy**.
5. Click **Create Policy**.
6. Under **Conditions | Applications Targeted**, click **Add Application Targeted**.
7. Search for and add the **Bash Homebrew File Specification Filter** previously created.

8. Click **Update**.
9. Click **Inclusions**.
10. Search for and add the **Homebrew Installer Commandline Filter** previously created.
11. Click **Update**.
12. Under **Actions**, click **Add Actions**.
13. Search for and add the **Homebrew Admin Group Membership Action** previously created.
14. Click **Update**.
15. Click **Save Changes**.



macOS Specific Policies

Once your macOS agent is registered, creating policies for your macOS machines follows a very similar process to creating policies for Windows machines in Privilege Manager. The main approach should be via the use of the Policy Wizard aided by the following:

1. Collect File Data – This enables Privilege Manager to recognize specific files and file types in your environment. The file data that you want to target with policies are called Events. All imported files can be viewed via **File Inventory**.
2. Create Filters – This step sorts important file data (Events) according to different criteria.
3. Create Policies – This step defines what
   a. Actions to perform on applications and
   b. Targets (Locations) for those actions.
4. Assign Filters to Policies – This step directs a Policy's actions to the appropriate Events happening on your network. This step also allows a Policy to be set to active.

5. Order your Policies based on priority level–Once your policies are created, the order they execute across your network matters. See the Policy Priority topic for more details.

In macOS, roles are bifurcated into two groups: Admins, and Users rather than by Group Policy Objects (GPO) found in Windows environments.

Actions Supported by macOS Agents (Kernel vs System Extensions)

The following actions are supported by macOS agents:

Action	KEXT	SYSEX	Versions	Usage
Allow Copy to /Applications/ Directory	Y	Y	10.5 - 11.1.x	Used to elevate installation of an Application Bundle to the /Applications folder via Drag-n-Drop to the Privilege Manager.app window. This action is deprecated and does not work with v11.2+ macOS agents.
Allow Package Installation	Y	Y	10.5+	Used to elevate installation of installer packages.
Application Approval Request (with Offline Fallback) Message Action	Y	Y	10.6+	
Application Approval Request (with ServiceNow Request Item Number) Message Action	Y	Y	10.5+	
Application Approval Request Message Action	Y	Y	10.5+	
Application Denied Message Action	Y	Y	10.5+	
Application Justification Message Action	Y	Y	10.5+	
Application Warning Message Action	Y	Y	10.5+	
Authorization DB Rights	N	Y	11.0+	Grants the specified right allowing an application to perform an elevated task.

Action	KEXT	SYSEX	Versions	Usage
Command Line Approval Message	N	Y	11.1+	
Command Line Justification Question	N	Y	11.1+	
Deny Execute	Y	Y	10.5+	
Deny Execute Message	Y	Y	10.5+	
Display User Message	Y	Y	10.5+	
File Quarantine	Y	Y	10.5+	
Just in Time Group Membership	N	Y	10.8.2+	
Run as Custom User	Y	N	10.5-10.8.2	
Run as Print Admin User	Y	N	10.5-10.8.2	
Run as Root	Y	N	10.5-10.8.2	
Run As User	N	Y	11.1+	

The following actions are specific to the use of sudo through our sudo plugin:

- Command Line Approval Message
- Command Line Justification Message
- Run As User

Agent Behavior with Actions

When a policy is used to manage .pkg installations on macOS endpoints with the Privilege Manager agent installed, you can expect the following behaviors:

Installation of a .pkg happens without prompting for credentials when

- the only action configured in the policy is **Allow Package Installation** or
- if any of the following are configured along with **Allow Package Installation**:
  - Application Approval Request Message Action
  - Application Approval Request (with Offline Fallback) Message Action
  - Approval Request (with ServiceNow Request Item Number) Form Action

- Application Justification Message Action
- Application Warning Message Action

A .pkg will NOT be installed if the only action is either of the following:

- Deny Execute
- Deny Execute + Deny Execute Message
- Application Denied Message Action

Any .pkg not managed by a Privilege Manager policy will be installed via the normal macOS workflow requiring admin credentials when prompted.

Inventory of Application Bundles

Privilege Manager allows the inventory of macOS application bundles. These are most likely applications already installed on a macOS system that can be found in the Applications folder. In order for Privilege Manager to inventory application bundles, the user needs to create a .zip file of the application bundles and move it outside of the Applications folder. Once the .zip is created and moved, it can be uploaded to Privilege Manager for inventory purposes.

A .zip of an application bundle when inventoried can contain one or more Mach-O binaries. The level of details that can be inventoried automatically depends on the format of and information provided in the Info.plist file.

The examples below show certain steps for the zip and upload process for one type of file, while the inventory examples are shown for

- a readable Info.plist file with an application bundle containing one Mach-O binary.
- a readable Info.plist file with an application bundle containing more than one Mach-O binary.
- a binary Info.plist file that does not provide sufficient details automatically and that will require manual steps to add information to the filter and/or policy.

The **Manage Application** option is only available on files inside the .zip compressed archives and not on the .zip file itself.

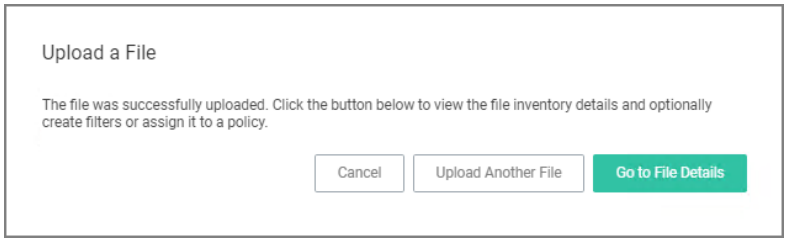
Creating a .zip File

1. Navigate to an application bundle file inside **/Applications**.
2. Right-click and select **Compress**.
3. Select the created .zip file and move it out of **/Applications**.

Uploading the .zip File

1. Use **Admin | File Upload** to start the inventory process.
2. Choose a file to upload and click **Upload File**.

3. After uploading a .zip file, click **Go to File Details**.



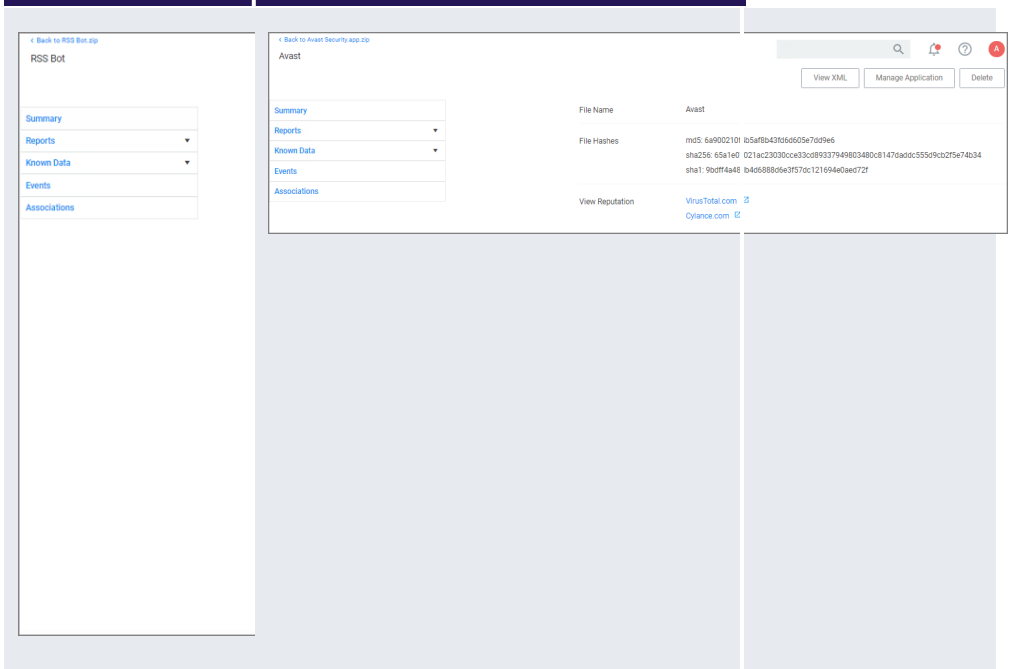
4. On the Resource Explorer page, view all the details available.

Creating a Filter from the Inventoried .zip File

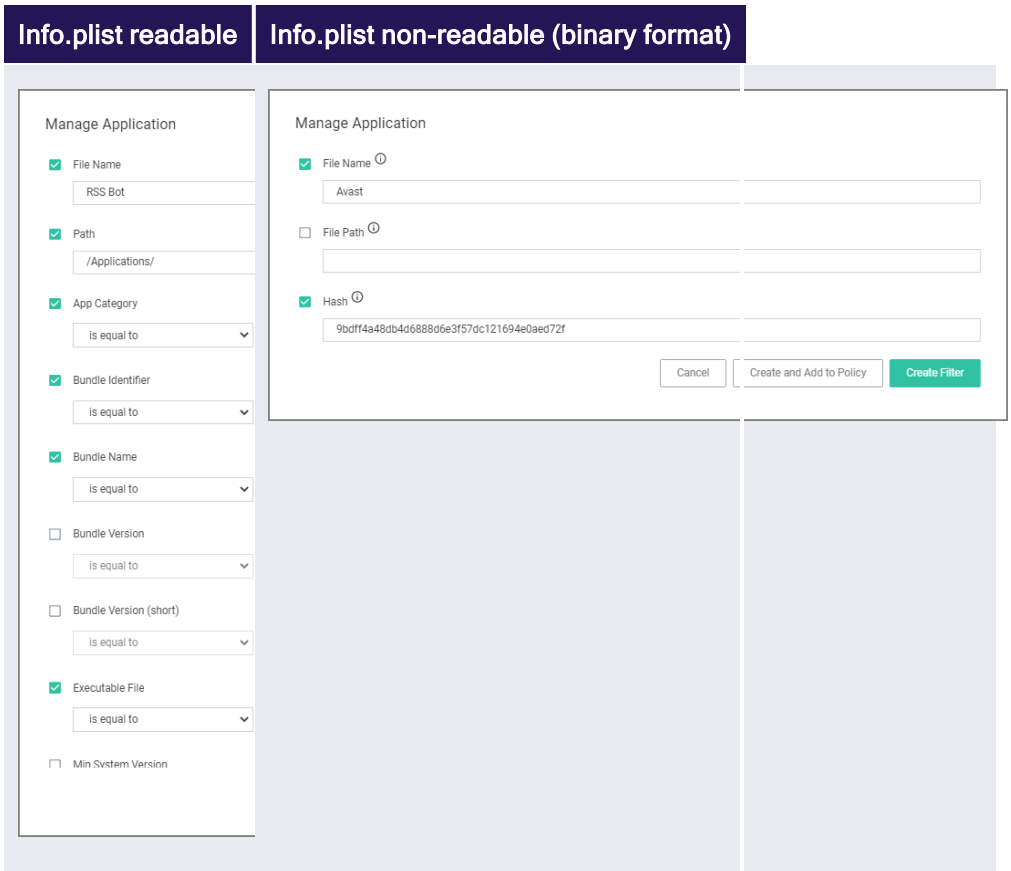
1. On the Resource Explorer page under **Known Data | File Inventory**, select **Virtual Disk File Contents**.

2. In the **File** column, click on the Mach-O binary name.
3. The Resource explorer is now displaying the information for the client item. The table below shows the difference between readable (left column) and non-readable (right column) Info.plist files.

Info.plist readable	Info.plist non-readable (binary format)



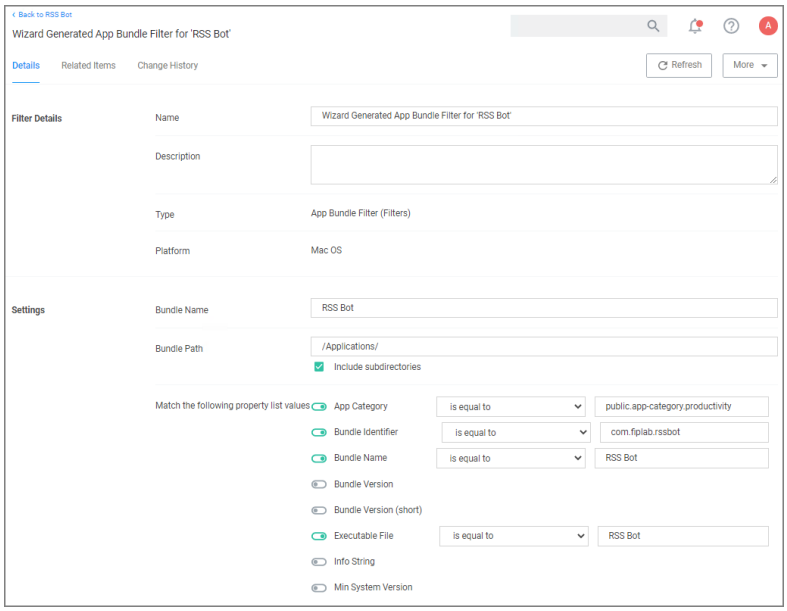
4. Click **Manage Application**.



Select any or all of the options on the Manage Application modal.

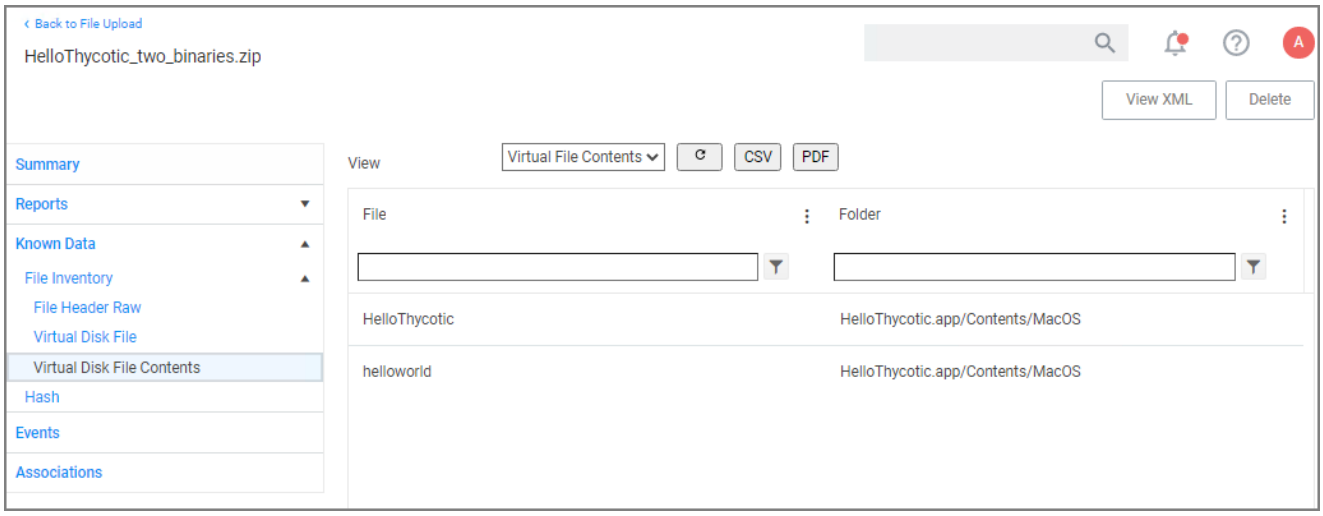
5. Click **Create Filter**.

   When dealing with an application bundle that has a readable Info.plist, Privilege Manager creates a very detailed *Wizard Generated App Bundle Filter* for the application bundle. This filter can be further customized and added to any policy.



Uploading a .zip with Two Mach-O Binaries

App bundles can contain more than one Mach-O binary, which will all be inventoried and accessible via the client items under **Known Data | Virtual Disk File Contents**:



While an application bundle can contain many binaries, you may want to only create an App Bundle filter for the binary set as the **CFBundleExecutable** in the Info.Plist. For some applications this may be sufficient, but you may need to create additional non-App Bundle filters for the other binaries.

App Bundle Contents Info.plist (binary format)

Depending on how the vendor created the application bundle, the level of detail to be inventoried might vary. Sometimes it is necessary to look at other artifacts in the bundle to customize the filter and or policy further.

For this we will look at an Info.plist file in binary format. For example,

- to manually add a Bundle Identifier to the filter, search for the tag `<CFBundleIdentifier>` and enter the string value in the appropriate filter field.
- to manually add a Bundle Version (short) to the filter, search for the tag `<CFBundleShortVersionString>` and enter the string value in the appropriate filter field.

Note: Reading an Info.plist file might depend on the tool that is being used. If opened in TextEdit only, they can appear garbled. On macOS systems, we recommend using QuickLock (⌘ Y), XCode, or something like Visual Studio Code. On Windows systems, we recommend Visual Studio Code or Notepad++.


```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://wwwapplicationle.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>BuildMachineOSBuild</key>
    <string>19G2021</string>
    <key>CFBundleDevelopmentRegion</key>
    <string>en</string>
    <key>CFBundleDisplayName</key>
    <string>Avast</string>
    <key>CFBundleDocumentTypes</key>
    <array>
        <dict>
            <key>CFBundleTypeName</key>
            <string>Any Item</string>
            <key>CFBundleTypeRole</key>
            <string>None</string>
            <key>LSHandlerRank</key>
            <string>None</string>
            <key>LSItemContentTypes</key>
            <array>
                <string>public.item</string>
            </array>
        </dict>
    </array>
    <key>CFBundleExecutable</key>
    <string>Avast</string>
    <key>CFBundleIconFile</key>
    <string>AppIcon</string>
    <key>CFBundleIdentifier</key>
    <string>com.avast.AAFM</string>
    <key>CFBundleInfoDictionaryVersion</key>
    <string>6.0</string>
    <key>CFBundleName</key>
    <string>Avast</string>
    <key>CFBundlePackageType</key>
    <string>APPL</string>
    <key>CFBundleShortVersionString</key>
    <string>14.9</string>
    <key>CFBundleSupportedPlatforms</key>
    <array>
        <string>MacOSX</string>
```

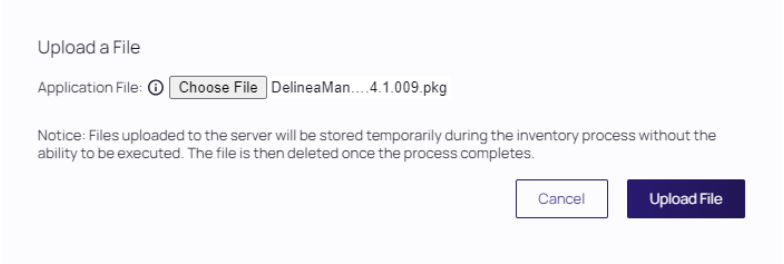
```
</array>
<key>CFBundleURLTypes</key>
<array>
    <dict>
        <key>CFBundleTypeRole</key>
        <string>Viewer</string>
        <key>CFBundleURLName</key>
        <string>com.avast.webdocument</string>
        <key>CFBundleURLSchemes</key>
        <array>
            <string>avastav</string>
        </array>
    </dict>
</array>
<key>CFBundleVersion</key>
<string>1</string>
<key>DTCompiler</key>
<string>comapplicationle.compilers.llvm.clang.1_0</string>
<key>DTPlatformBuild</key>
<string>12B45b</string>
<key>DTPlatformName</key>
<string>macosx</string>
<key>DTPlatformVersion</key>
<string>11.0</string>
<key>DTSDKBuild</key>
<string>20A2408</string>
<key>DTSDKName</key>
<string>macosx11.0</string>
<key>DTXcode</key>
<string>1220</string>
<key>DTXcodeBuild</key>
<string>12B45b</string>
<key>LSMinimumSystemVersion</key>
<string>10.10</string>
<key>LSUIElement</key>
<true/>
<key>NSCameraUsageDescription</key>
<string>Change Avast Omni profile picture</string>
<key>NSHumanReadableCopyright</key>
<string>Copyright © 2021 AVAST Software s.r.o. All rights reserved.</string>
<key>NSMainNibFile</key>
<string>MainMenu</string>
<key>NSPrincipalClass</key>
<string>Avast.AntivirusModule</string>
<key>NSServices</key>
<array>
    <dict>
        <key>NSMenuItem</key>
        <dict>
            <key>default</key>
            <string>Scan with Avast</string>
        </dict>
        <key>NSMessage</key>
```

```
            <string>scanFromServicesMenu</string>
            <key>NSPortName</key>
            <string>Avast</string>
            <key>NSRequiredContext</key>
            <dict>
                <key>NSApplicationIdentifier</key>
                <string>comapplicationle.finder</string>
            </dict>
            <key>NSSendFileTypes</key>
            <array>
                <string>public.item</string>
            </array>
            <key>NSServiceDescription</key>
            <string>ScanServicesDesc</string>
        </dict>
    </array>
</dict>
</plist>
```

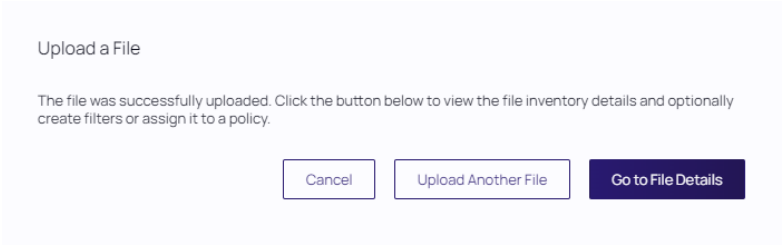
Inventorying .pkg Files

Privilege Manager allows the inventory of macOS .pkg files. With the ability to upload and extract the contents within the .pkg files, Privilege Manager inventories the applications that are bundled in any given .pkg, however, it is useful to note that not all .pkg files will be bundles.

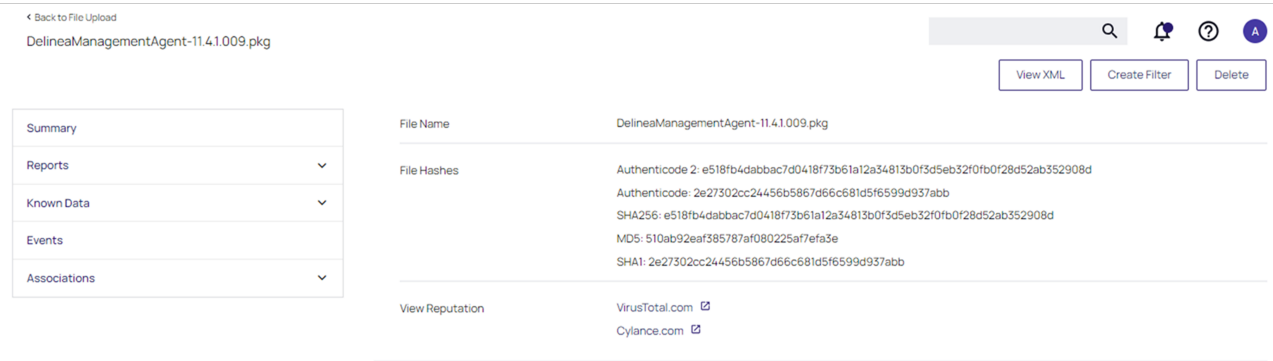
1. Use **Admin | File Upload** to start the inventory process.
2. Choose a file to upload and click **Upload File**.



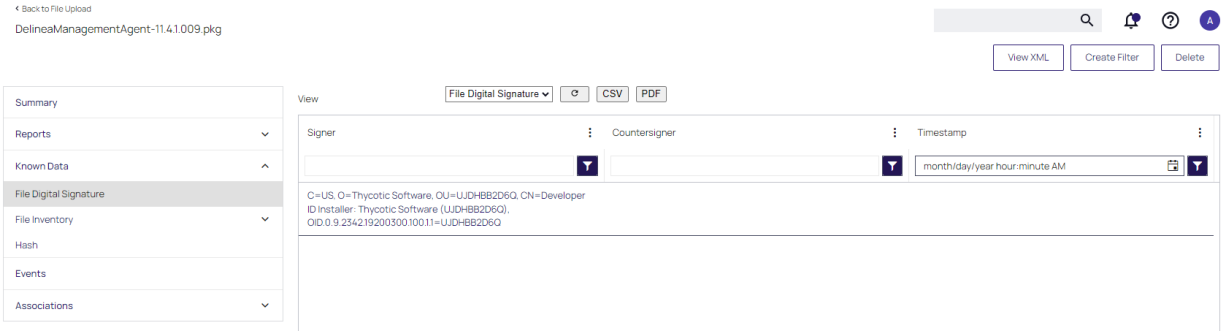
3. After uploading a .pkg file select the **Go to File Details** button.



In the Resource Explorer, an Administrator can now look at all the details from the inventory, showing the Summary.



4. Click **Known Data** to see the information specified in the macOS bundle. This includes information such as:
   - **File Digital Signature**: includes the Signing certificate CN and Signing team ID
   - **File Inventory**: includes the Raw file header, contents of the .pkg file, and package summary (title and version)
   - **Hash**: Hash values of the uploaded .pkg file as defined under inventory hash algorithm(s)



Note: Any packages that deviate from the standard configuration and layout might not have their contents inventoried correctly. In that case, unpack the .pkg and upload each contents file individually for inventory purposes.

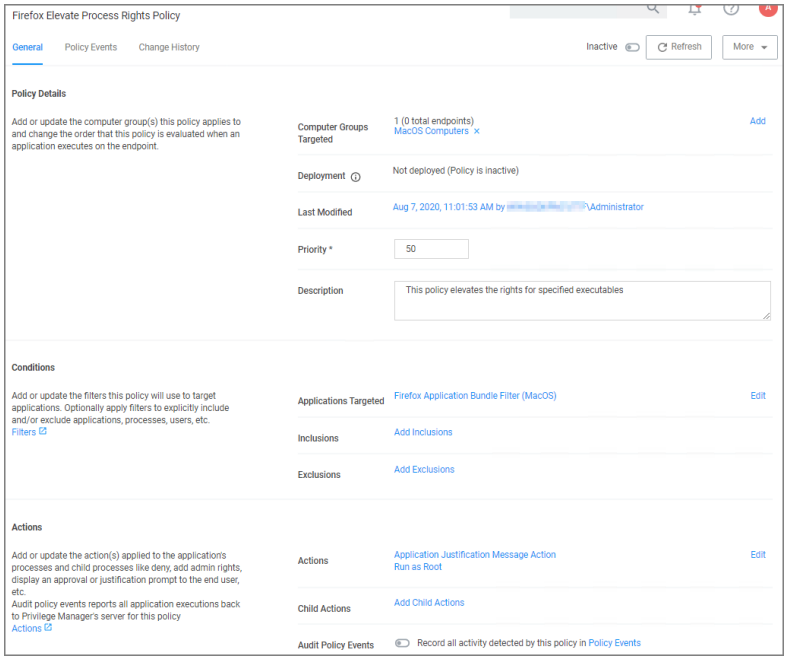
Require Justification - FireFox

The following example provides information on setting up a justification required policy for FireFox on a macOS workstation. This policy is supported for all agent types.

Create a filter for Firefox either from discovery, refer to File Inventory or manually, refer to Creating a Filter Manually. Use that filter in the steps below.

1. Using the Policy Wizard, create a controlling policy, click **Next Step**.
2. Select **Elevate**, click **Next Step**.
3. Select **Require Justification**, and click **Next Step**.

4. Select what file type to target, for this example select **Executable**, and click **Next Step**.
5. Choose your target, for this example **Existing Filter**.
6. Search for and add your Firefox filter.
7. Click **Updated**.
8. Click **Next Step**.
9. Name your policy and add a description, click **Create Policy**.

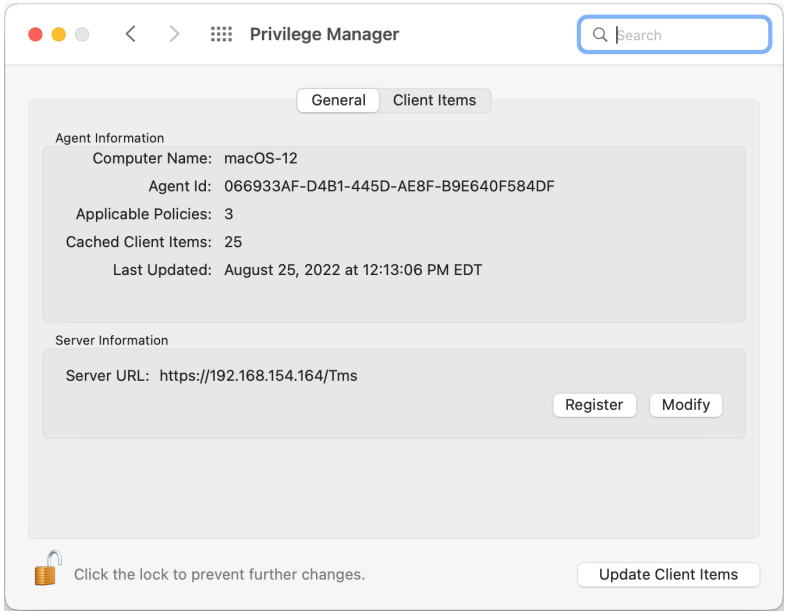


10. Set the **Inactive** switch to **Active**.

Updating the Workstation

On the macOS workstation,

1. Open **System Preferences | Privilege Manager**.

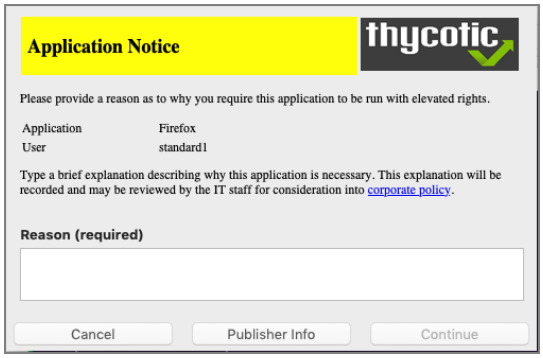


2. Click **Update Client Items**.

The agent updates with new and updated policies and synchronizes.

Expected User Experience

Once the justification policy is updated on an endpoint, when users click Firefox they will see a prompt to enter their justification reason for accessing Firefox.



Move to Trash Bin Policy

When a standard user deletes an application bundle via ⌘ **-delete** or **drag-n-drop** from /Applications, the following actions are taken based on policy evaluation:

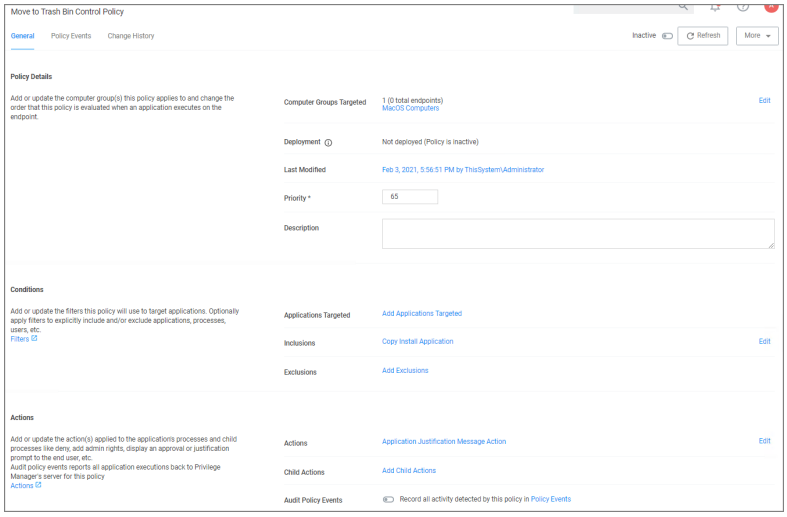
- Allow - Is allowed without prompting user for credentials
- Present appropriate Advanced Message Dialog:

- Approval - Approval process is invoked before it is allowed to complete
  - Cancelled - It is denied.
- Denied - Denied dialog is invoked and user can not delete the application bundle
- Justification - Justification process is invoked before it is allowed to complete
  - Cancelled - It is denied.
- Offline-Approval - Offline-approval process is invoked before it is allowed to complete
  - Cancelled - It is denied.
- Warning - Warning dialog is invoked before it is allowed to complete
  - Cancelled - It is denied.

To allow a standard user to delete application bundles from the /Applications directory, create an elevation policy that uses the **Copy Install Application** filter under Inclusions. We recommend to also add a justification message action. If used on endpoints running the **KEXT** agent, the policy needs to target an application to work correctly. For this example we are starting with an empty policy.

1. Navigate to your macOS Computer Group and select **Application Policies**.
2. Click **Create Policy**.
3. Click **Skip the wizard, take me to a blank policy**.
4. Enter a Name and description for your policy, click **Create Policy**.
5. Click **Add Inclusions**.
6. Search for and add the **Copy Install Application** filter.
7. Click **Update**.
8. Click **Add Actions**.
9. Search for and add the **Application Justification Message Action**.
10. Click **Update**.
11. Click **Save Changes**.

12. Set the **Inactive** switch to **Active** for policy updates at the endpoint.



Note: A policy configured in this way will also allow a user to update or replace an App Bundle by drag-n-drop via Finder to the /Applications folder.

Application Self-elevation

Important: The Finder Sync Extension is deprecated with release version 11.2+. This feature is only available with the KEXT based Privilege Manager Agent. Self-elevation in this form is not possible with the system extension.

Refer to previous documentation versions for details about the Finder Sync Extension setup for KEXT based Privilege Manager agents.

Targeting .pkg Files

Privilege Manager supports elevation of an installation package (also known as a package). A package contains a product or product component—the package's payload—to be installed on a computer and install configuration information that determines where and how the product is installed. A package is often identified by the file extension of *.pkg* or *.mpkg*.

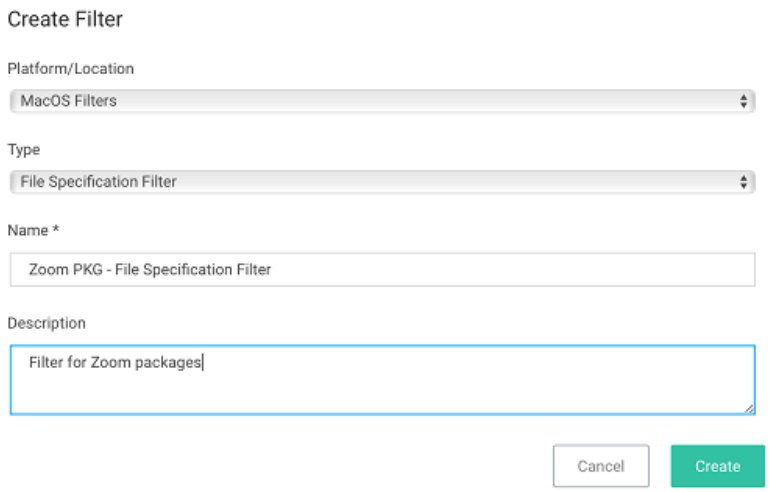
You can use the Policy Wizard to create policies that apply to packages or you can create them manually. This document details how to create a policy manually.

For this example, we'll be using a file specification filter for the file "Zoom.pkg". To be more granular, you could use a file hash filter that targets the desired algorithm for the package file. Signed file filters are not supported for packages at this time.

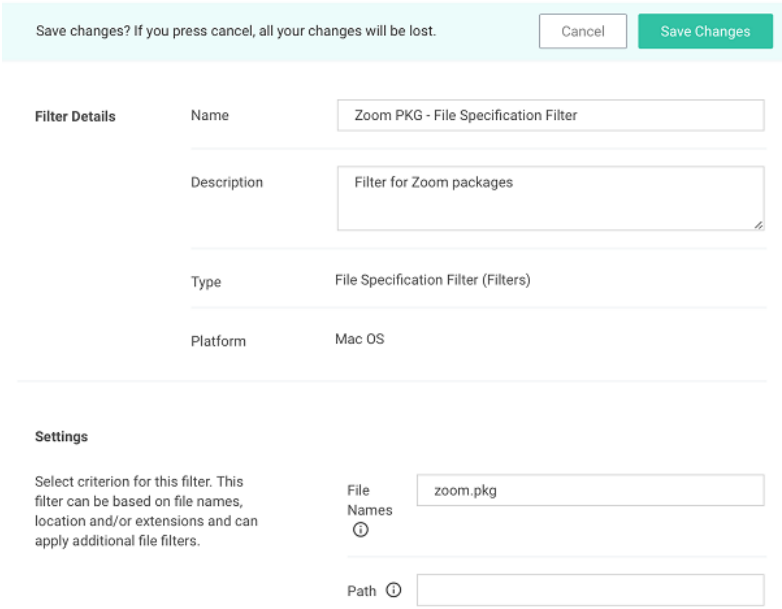
Create File Specification Filter for the Package

1. Navigate to **Admin | Filters**
2. Click **Create Filter**
3. For Platform/Location, pick **macOS Computer Filters**

4. For Type, pick **File Specification Filter**
5. Give the filter a name and description and click **Create**



6. Set File Names to *zoom.pkg* and click **Save Changes**



Create Policy Targeting File Specification Filter

1. Navigate to **MACOS Computers | Application Policies**
2. Click **Create Policy**
3. Click **Skip the wizard, take me to a blank policy**
4. Give the policy a name and description and click **Create Policy**

5. Set **Applications Targeted** to the file specification filter you created for the package
6. Set **Inclusions** to **Privilege Manager Copy/Installer Helper Parent Process Filter**
7. Actions – Depending on the desired user experience, use the following combinations of actions:

Actions	Outcome
Deny Execute	Package installation is denied.
Deny Execute Deny Execute Message	Package installation is denied and a notification is posted in notification center.
Application Denied Message Action (HTML)	Package installation is denied and the custom Application Denied Message Action (HTML) dialog is displayed.
Allow Package Installation	Package installation is allowed without prompting the user for admin credentials.
Allow Package Installation Application Approval Request Message Action (HTML)	Package installation is allowed after the user's approval request has been approved. ^
Allow Package Installation Application Approval Request (with Offline Fallback) Message Action	Package installation is allowed after the user's approval request has been approved. ^
Allow Package Installation Application Justification Message Action (HTML)	Package installation is allowed after the user enters a justification.
Allow Package Installation Application Warning Message Action (HTML)	Package installation is allowed after the user acknowledges the warning dialog.

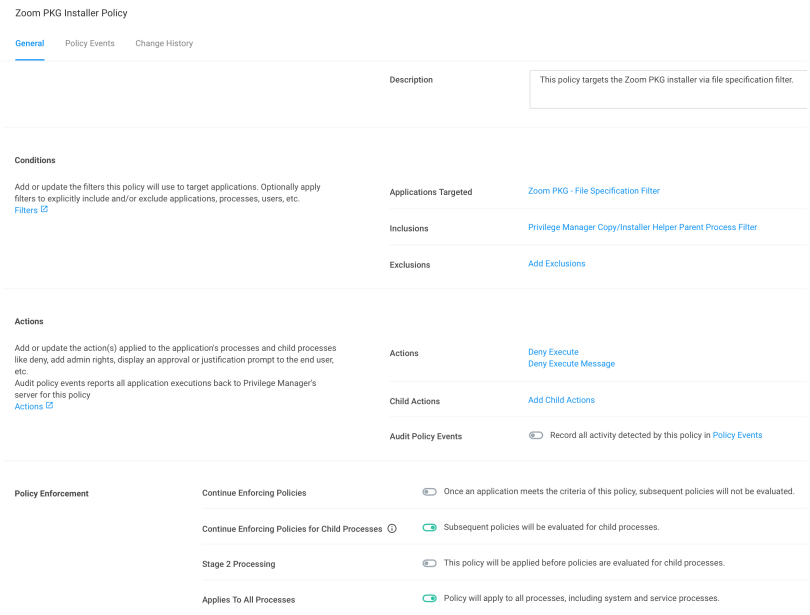
^ If the request is denied, a notification will be posted in notification center.

8. Click **Show Advanced**
   - Click **Continue Enforcing Policies** so that it is disabled
   - Click **Applies To All Process** so that it is enabled
9. Click **Save Changes**
10. Set the policy as **Active**

Policy Examples

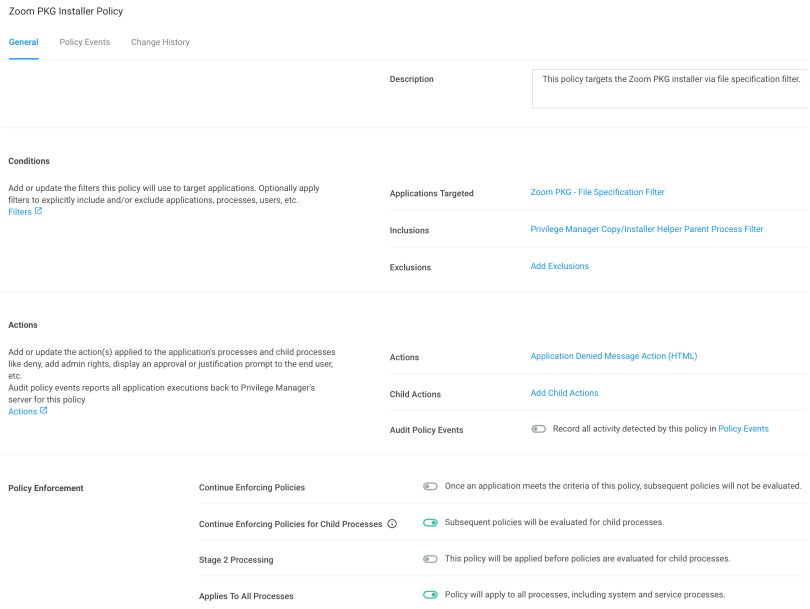
Deny Execute + Deny Execute Message

The Policy below will deny package installation and a notification is posted in notification center.



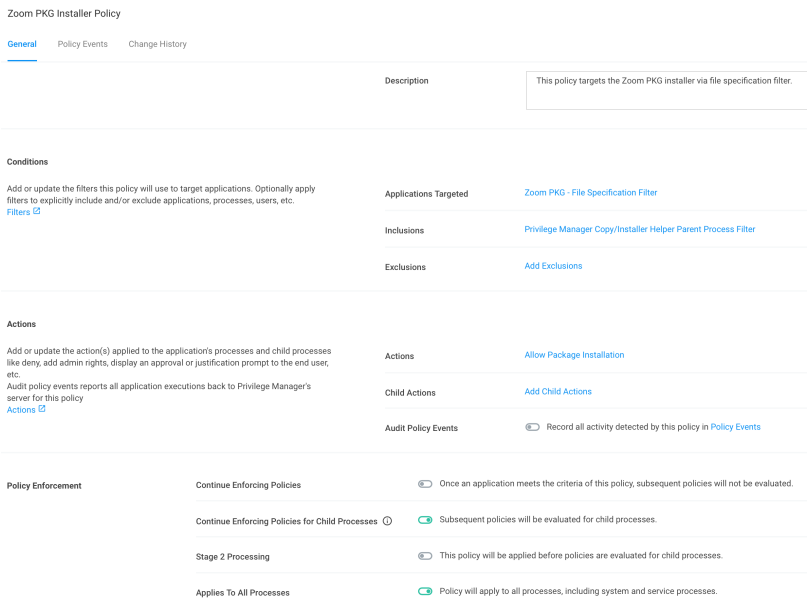
Application Denied Message Action (HTML)

The Policy below will deny the package installation and the custom Application Denied Message Action (HTML) dialog is displayed.



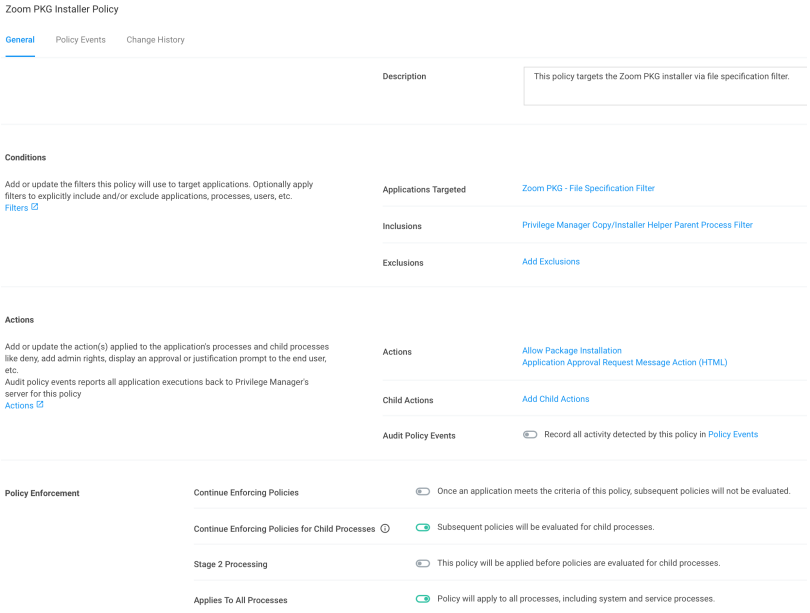
Allow Package Installation

The Policy below will allow package installation without prompting the user for admin credentials.



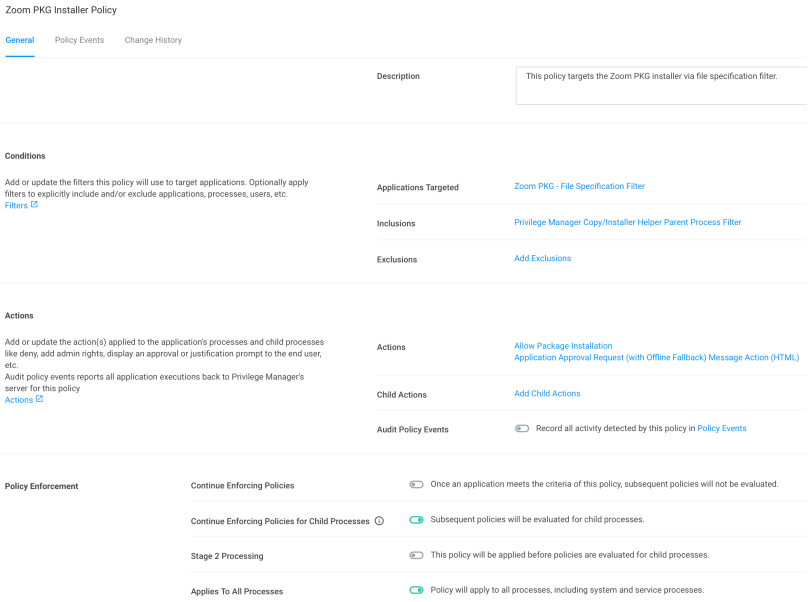
Allow Package Installation + Application Approval Request Message Action (HTML)

The Policy below will allow package installation after the user's approval request has been approved. If the request is denied, a notification will be posted in notification center.



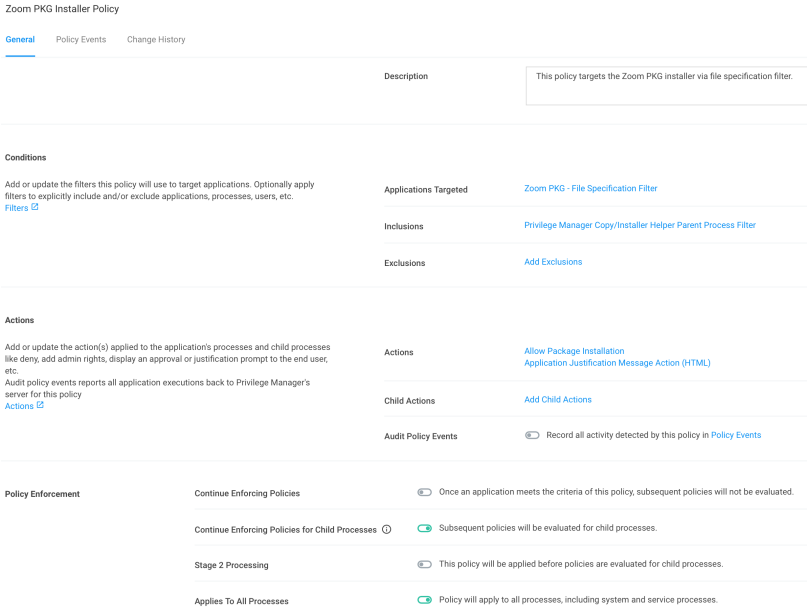
Allow Package Installation + Application Approval Request (with Offline Fallback) Message Action (HTML)

The Policy below will allow package installation after the user's approval request has been approved. If the request is denied, a notification will be posted in notification center.



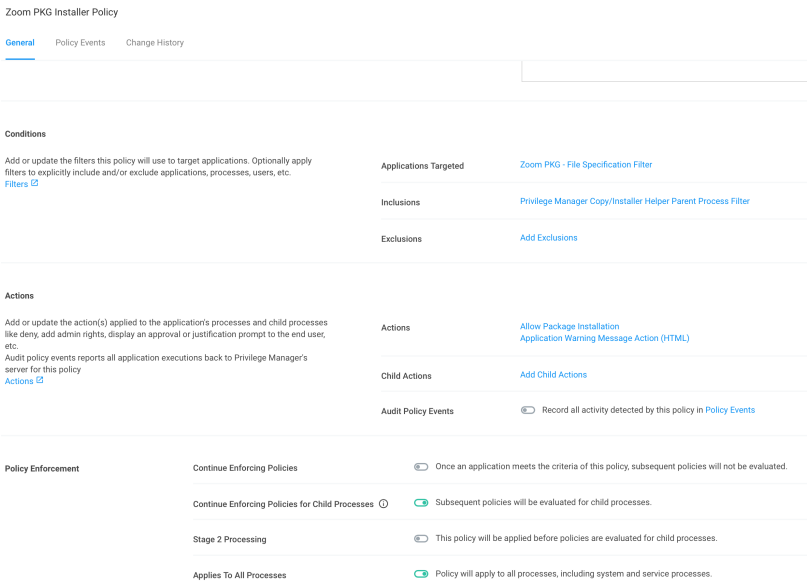
Allow Package Installation + Application Justification Message Action (HTML)

The Policy below will allow package installation after the user enters a justification.



Allow Package Installation + Application Warning Message Action (HTML)

The Policy below will allow package installation after the user acknowledges the warning dialog.



Controlling the Usage of sudo

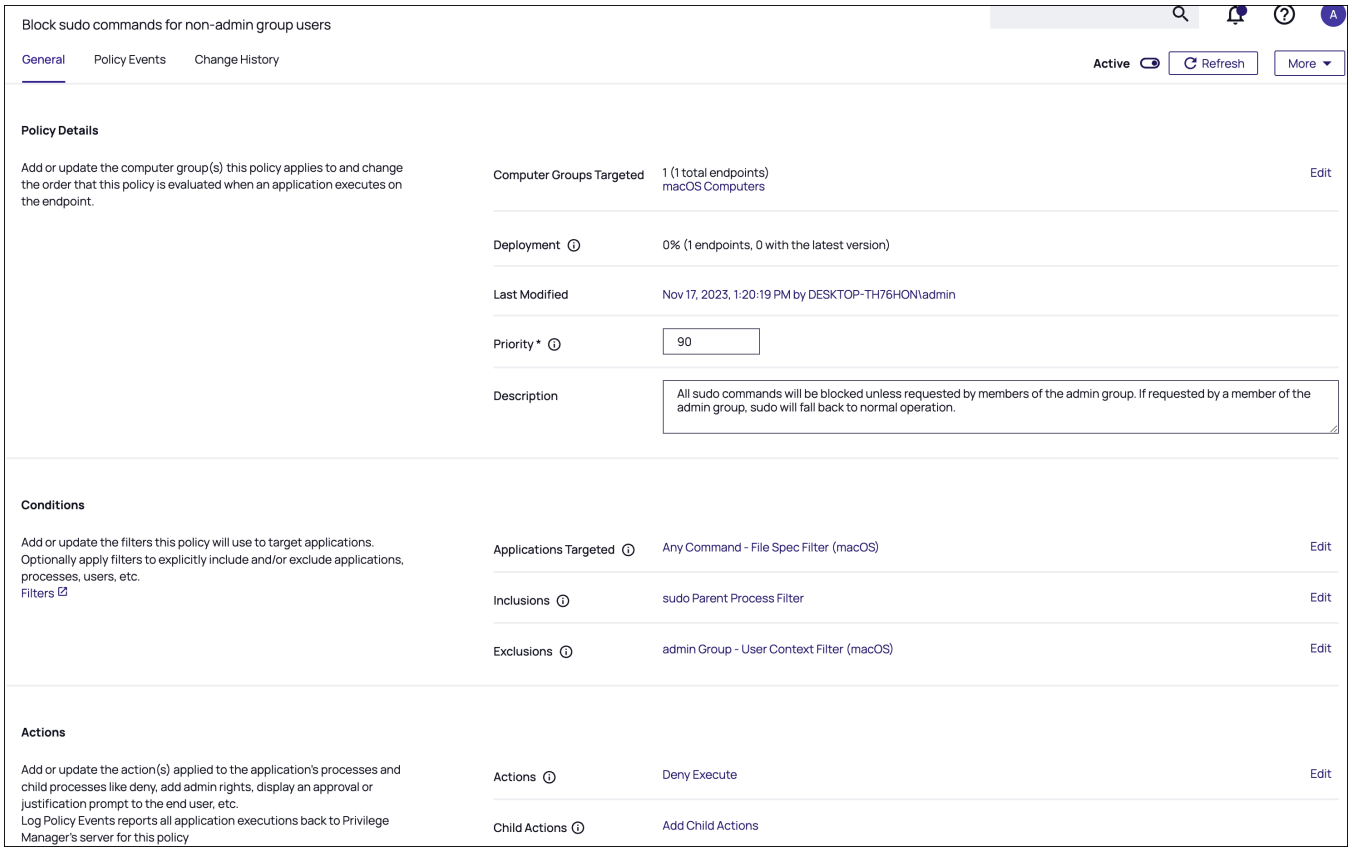
Privilege Manager provides you with Workstation policies, that are foundation policies for rapid deployment. They are accessed from the Application Policies in your Computer Group. Click **Create Policy**, then select **Workstation Policies**. Refer to "Workstation Policies" on page 251

These specific Workstation policies provide ways of controlling how users can execute the sudo command. They are:

- **Block sudo Commands for Non-Admin Group Users**
- **Elevate sudo pmagentctl updateclientitems**

Configuring Block sudo commands for non-admin group users

First, let's look at the **Block sudo commands for non-admin group users** policy. This policy will block all sudo commands for users that are not a part of the Admin group. If a user is a part of the Admin group, sudo will fall back to normal operation.



In the **Applications Targeted** field, you see **Any Command - File Spec Filter (macOS)**. This filter will match on any command that a user can run.

In the **Inclusions** list, **sudo Parent Process Filter** appears as a filter that must match for the policy to apply. This means that this policy will apply to processes where sudo is the parent of the process. In more simple terms, this means that this policy will apply to commands run with sudo.

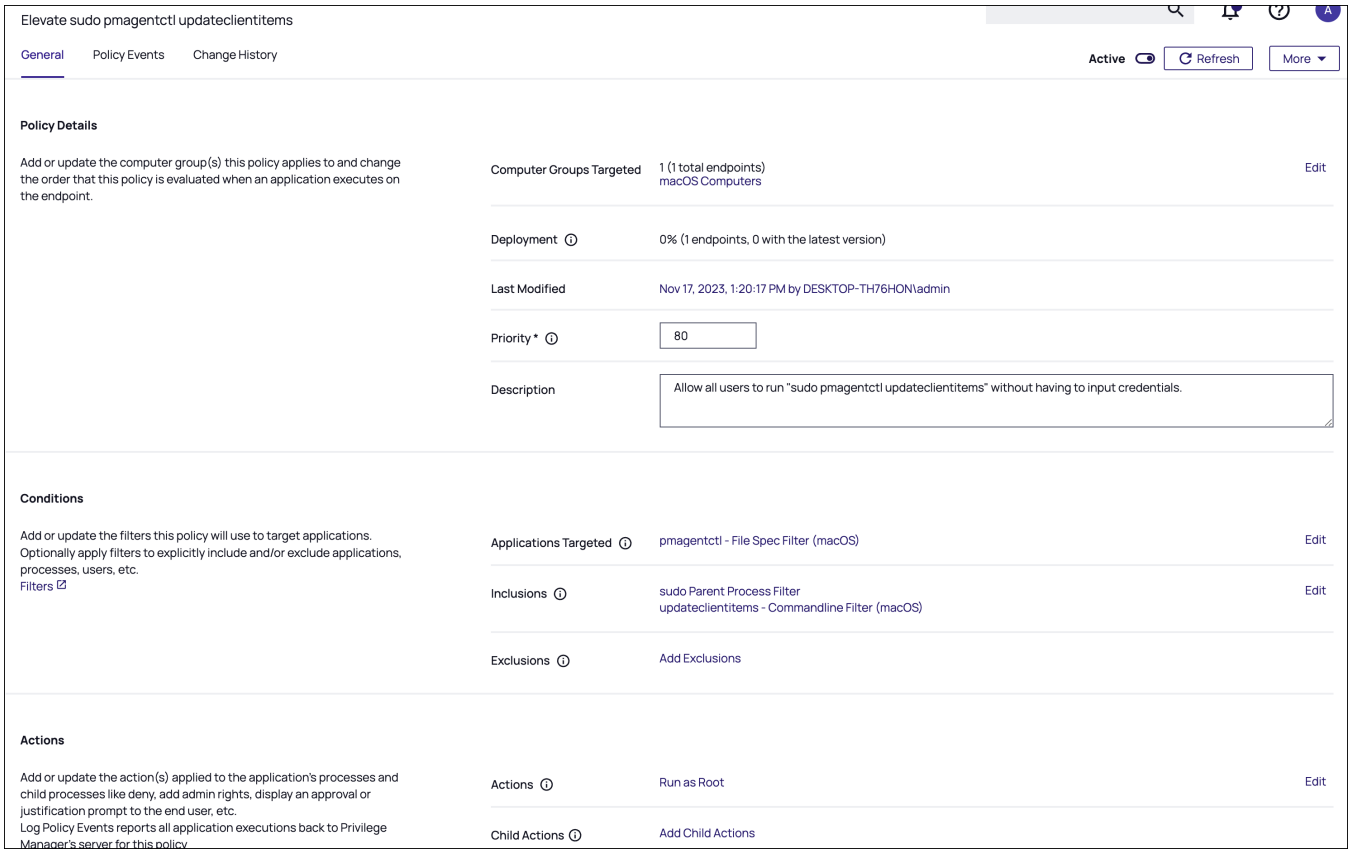
If we put the **Any Command - File Spec Filter (macOS)** and the **sudo Parent Process Filter** logic together, this means that the policy will match on any command that a user could run, if and only if that command is run with sudo.

Now, you see that **admin Group - User Context Filter (macOS)** is included in the **Exclusions** list as a filter that must not match for this policy to apply. This filter will match on macOS users in the Admin group. Since this filter is excluded, this policy will not apply to users in the Admin group.

Putting this all together, this policy blocks users that are not in the admin group from running any sudo commands.

Configuring Elevate sudo pmagentctl updateclientitems

Now, let's look at the next policy **Elevate sudo pmagentctl updateclientitems**. This policy allows users to run `sudo pmagentctl updateclientitems` in the Terminal without having to input credentials. See "Terminal Commands" on page 197 for more information on `pmagentctl`.



Again, you see that **sudo Parent Process Filter** is listed as an **Inclusion** and we know from the previous policy that this means that the policy will apply to commands run with sudo.

> **Note:** You will see a pattern here. When you want to control the usage of sudo, you need the **sudo Parent Process Filter** listed in the **Inclusions**.

In **Applications Targeted** field, **pmagentctl - File Spec Filter (macOS)** is listed. This filter targets the Privilege Manager macOS agent's command line utility **pmagentctl**.

There is another filter listed in the **Inclusion** section of this policy, **updateclientitems - Commandline Filter (macOS)**. As it sounds, this filter targets the command line `updateclientitems` which is a subcommand of `pmagentctl`.

Now, putting this all together, this policy is targeting `pmagentctl updateclientitems` when run with sudo.

These two Workstation policies can be applied alone or together. If they are applied together, **Elevate sudo pmagentctl updateclientitems** will apply before **Block sudo commands for non-admin group users** due to their priority. All users will be allowed to run `sudo pmagentctl updateclientitems` without having to input credentials. All other sudo commands will be blocked for non-Admin group users. For Admin group users, all other sudo commands will fall back to normal operation.

Summary

Now that we have explored these example policies, let's recap:

- If you want to control the usage of sudo, the **sudo Parent Process Filter** needs to be added to the Inclusions.
- You can target whatever application that can be run with sudo. In these examples, we targeted **Any Command - File Spec Filter (macOS)** and **pmagentctl - File Spec Filter (macOS)**.
- You can add filters to the **Inclusions** and **Exclusions** sections of a policy to filter on specific command lines. Refer to the example in "Configuring Elevate sudo pmagentctl updateclientitems" on page 391.

  You can also filter on users or groups here; we excluded the Admin group in the **Block sudo commands for non-admin group users** policy so Admin users could still run sudo commands if they input credentials. Refer to the example in "Configuring Block sudo commands for non-admin group users" on page 390.

  Note: This is not an exhaustive list of filters that can be added to the **Inclusions** and **Exclusions** sections.

- In these examples we have used **Deny Execute** or **Run as Root** in the actions to block or elevate sudo usage. More or different actions can be added here.
- It also must be noted that because we are dealing with command line tools, the **Applies to All Processes** option in the **Advanced Settings** is the only option that needs to be checked.

macOS Policy Wizard

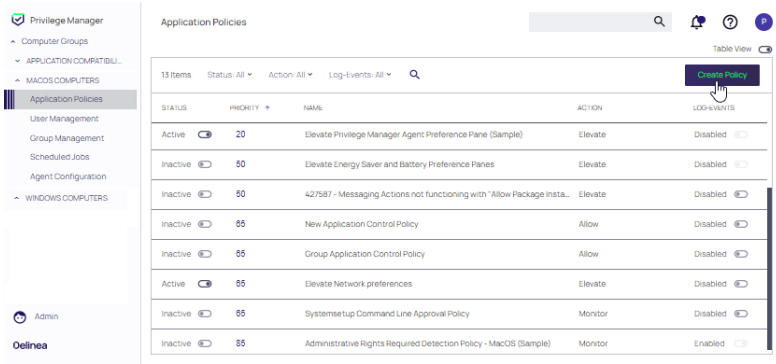
This section contains macOS policy wizard decision flow diagrams for controlling policies.

The following diagrams are available:

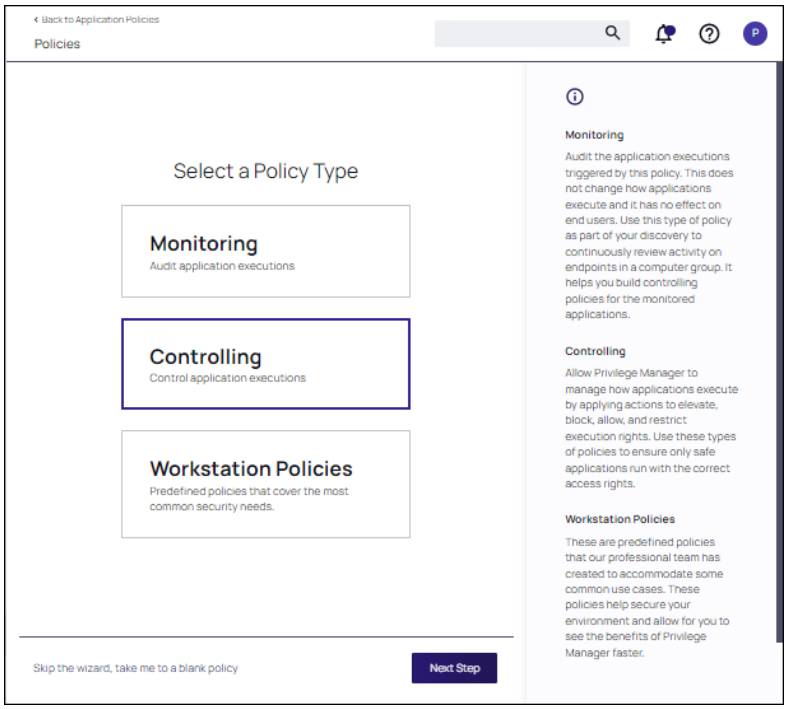
- Creating a Controlling Elevation Policy for macOS
- Creating a Controlling Allow Policy for macOS
- Creating a Controlling Block Policy for macOS

Creating a Controlling Allow Policy for macOS

1. For any of your Computer Groups navigate to **Application Policies**.

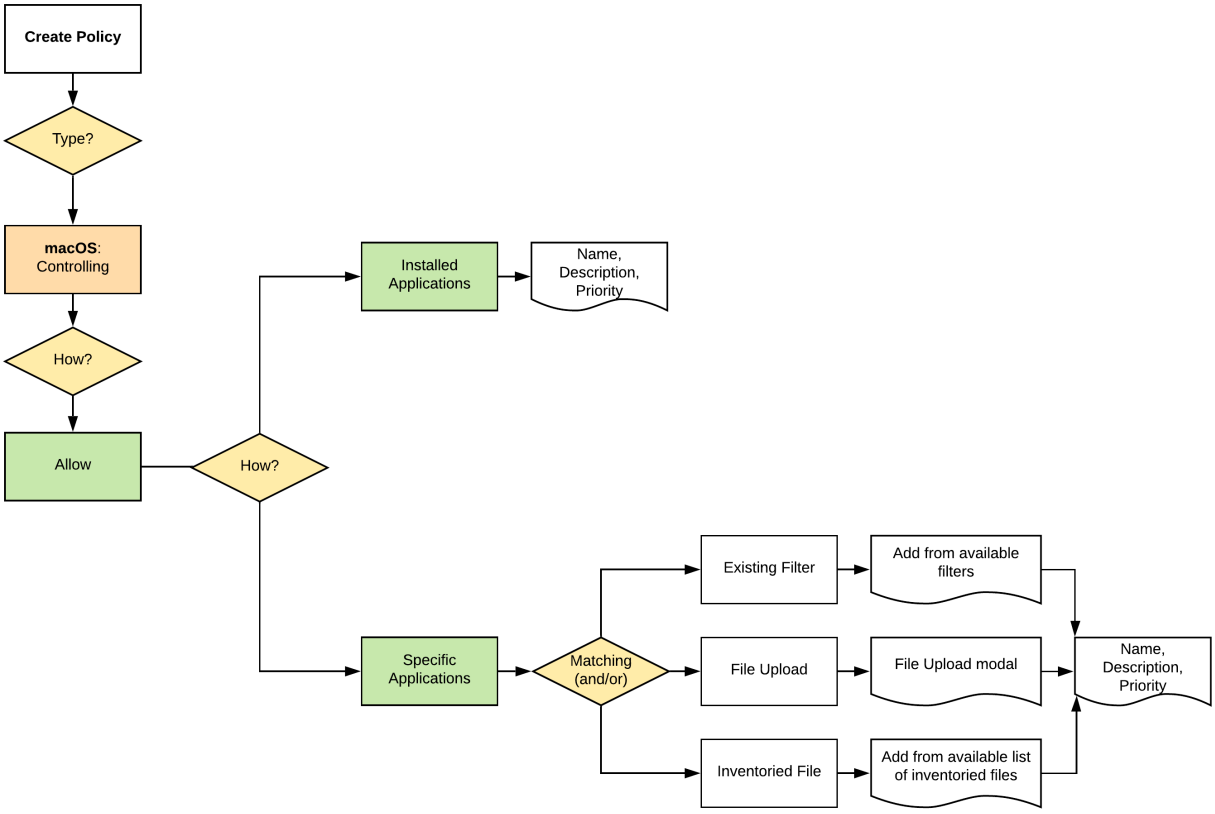


2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:



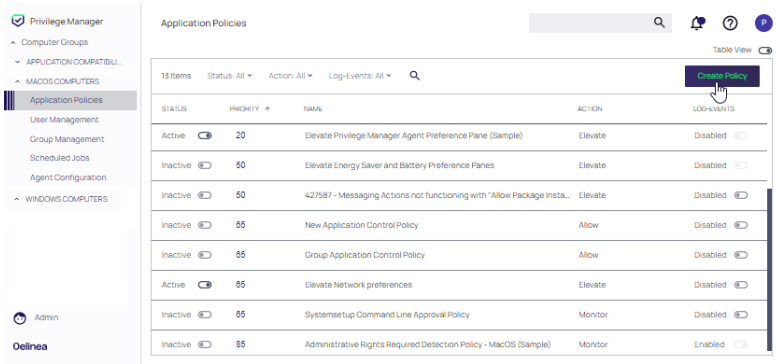
3. After assigning a name, description and verifying the priority number, click **Create Policy**.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

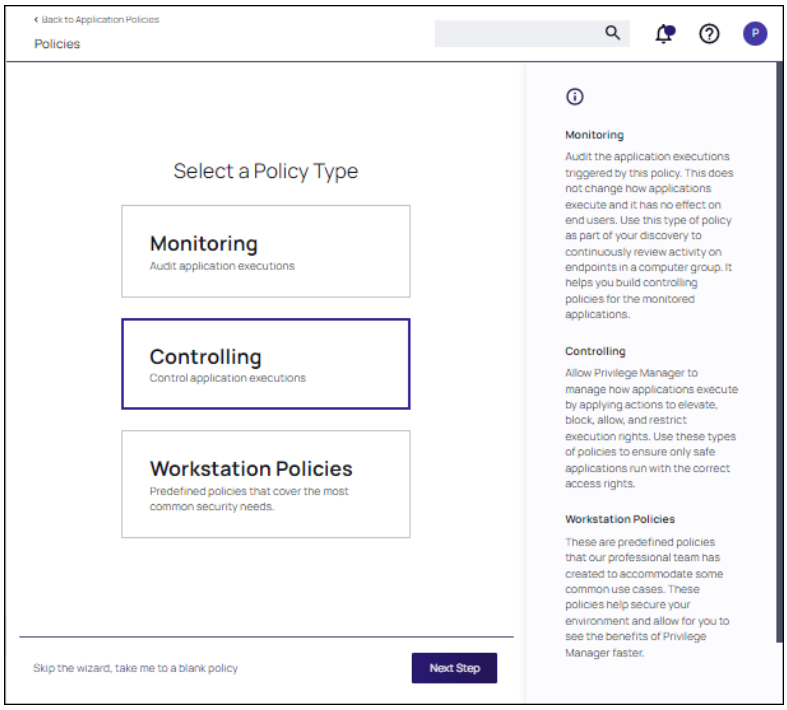
The wizard provides on page help explaining the different options available to the user.

Creating a Controlling Block Policy for macOS

1. For any of your Computer Groups navigate to **Application Policies**.

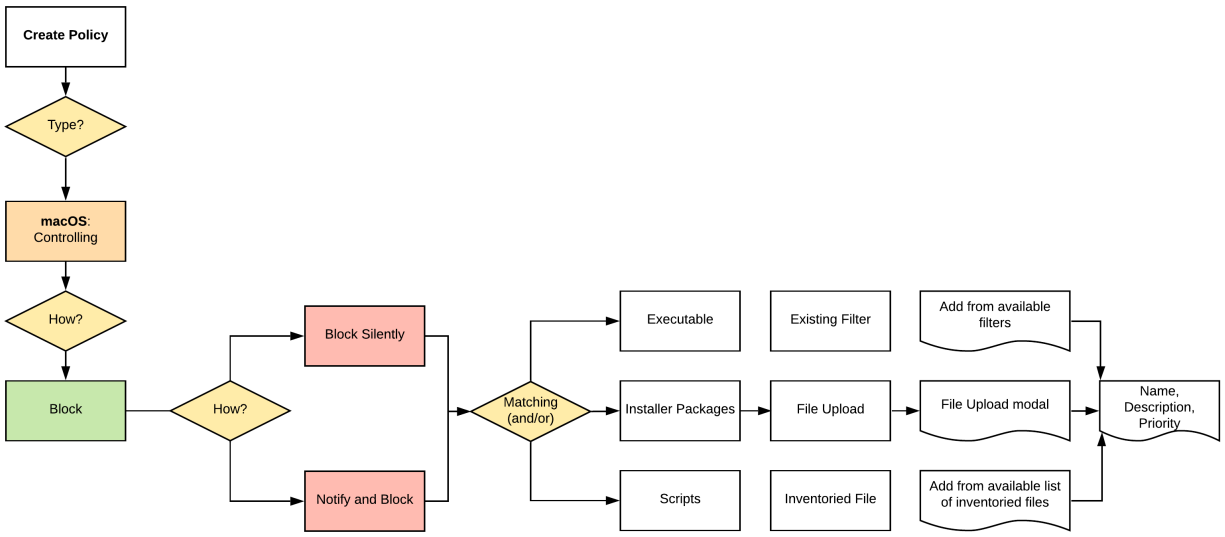


2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:



3. After assigning a name, description and verifying the priority number, click **Create Policy**.

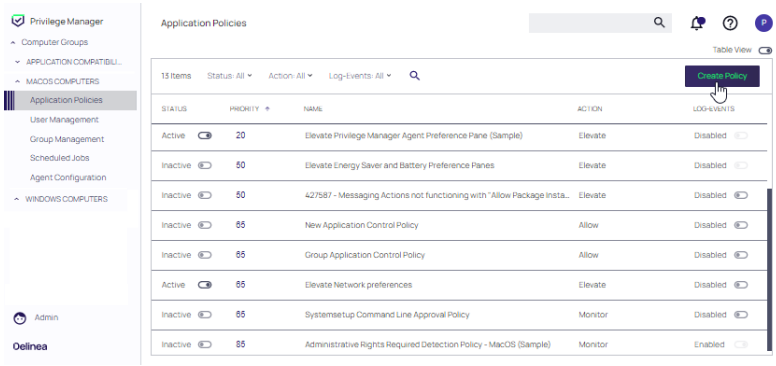
While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

The wizard provides on page help explaining the different options available to the user.

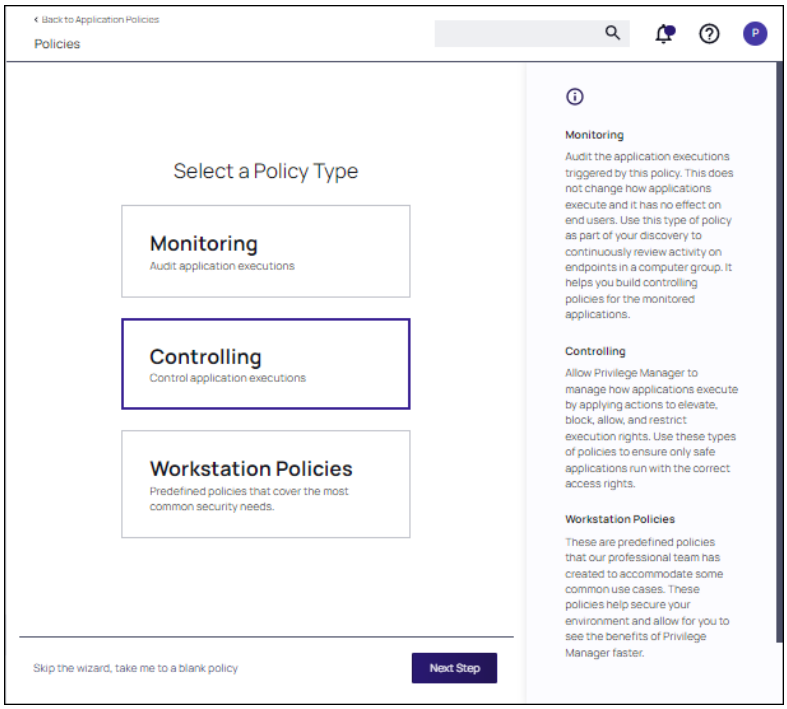
Creating a Controlling Elevation Policy for macOS

Note: The diagram shows actions "Run as Root" and "Just in Time" which will only work with the system extension based agent introduced with Privilege Manager v10.8.2.

1. For any of your Computer Groups navigate to **Application Policies**.



2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:

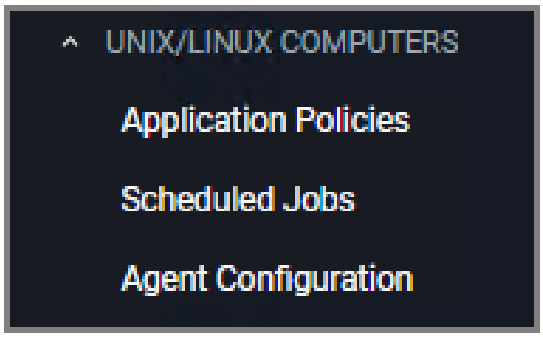
3. After assigning a name, description and verifying the priority number, click **Create Policy**.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

The wizard provides on page help explaining the different options available to the user.

Unix/Linux Computers

The default Unix/Linux Computer Group.



Note: Privilege Manager for Linux/Unix and Windows for servers is End of Sale/Renewal only.

This is the navigation entry point into the Unix/Linux Computer Group. The sub nodes are in feature parity with other OS computer groups. except for User and Group Management, which is not currently covered. All policies or resources underneath **UNIX/LINUX COMPUTERS** pertain to that specific default computer group.

For Unix/Linux Agent Configuration information refer to Agent Configuration.

Note: Linux/Unix user and group management is not enabled. The Unix/Linux agent allows administrators to get lists and details of local users, groups, and membership.

Unix/Linux Specific Policies

Note: Privilege Manager for Linux/Unix and Windows for servers is End of Sale/Renewal only.

Once your Unix/Linux agent is registered, creating policies for your Unix/Linux machines follows a very similar process to creating policies for Windows machines in Privilege Manager. The main approach should be via the use of the Policy Wizard aided by the following:

1. **Collect File Data**: This enables Privilege Manager to recognize specific files and file types in your environment. The file data that you want to target with policies are called Events. All imported files can be viewed via **File Inventory**.
2. **Create Filters**: This step sorts important file data (Events) according to different criteria.
3. **Create Policies**: This step defines what
   a. Actions to perform on applications and
   b. Targets (Locations) for those actions.

   Refer to the "Creating Policies" on page 241 topic.
4. **Assign Filters to Policies**: This step directs a Policy's actions to the appropriate Events happening on your network. This step also allows a Policy to be set to active.
5. **Order your Policies** based on priority level–Once your policies are created, the order they execute across your network matters. See the "Policy Priority" on page 269 topic for more details.

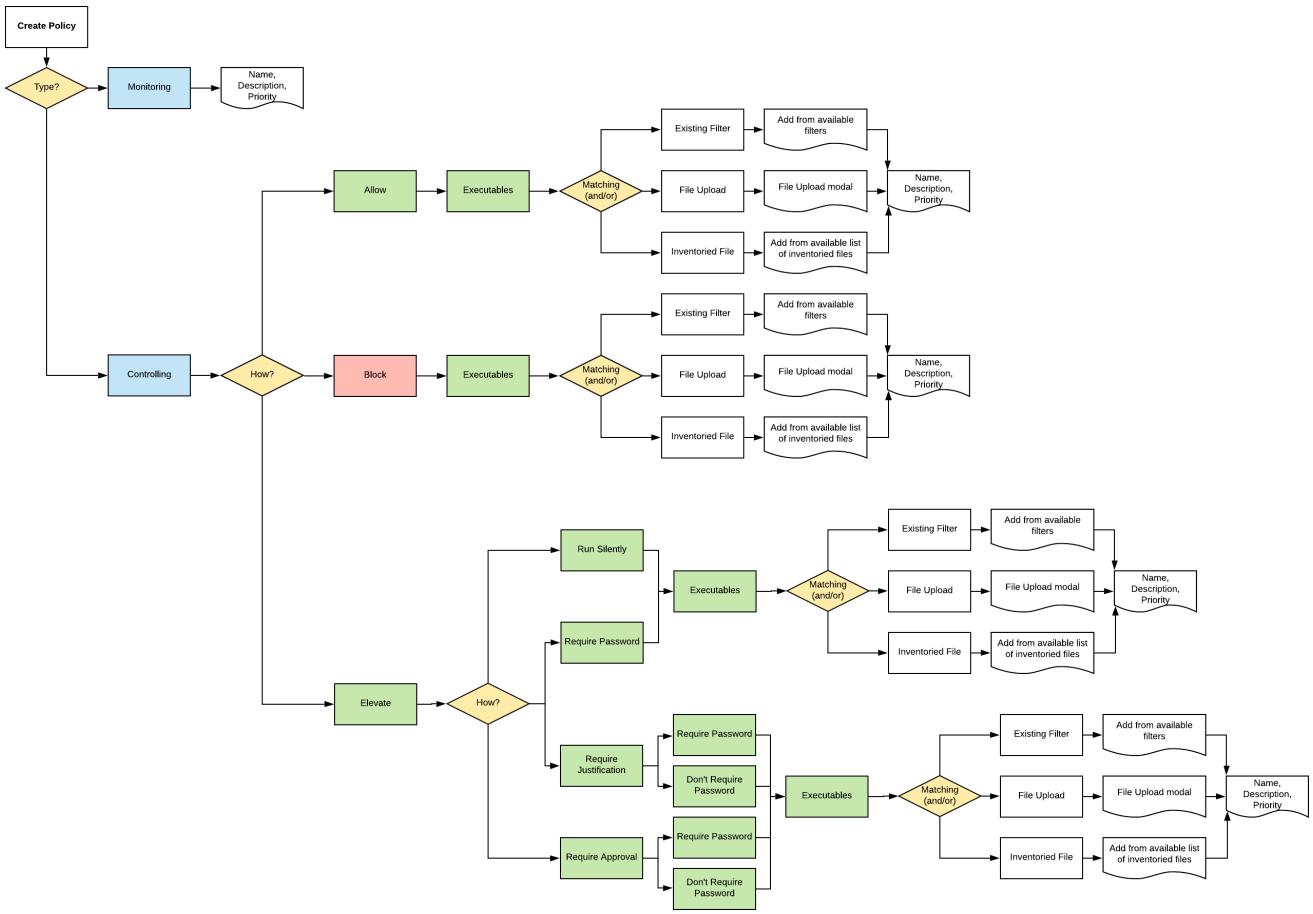
> **Note:** In Unix/Linux, roles are bifurcated into two groups: Admins, and Users rather than by Group Policy Objects (GPO) found in Windows environments.

Example Policies

- "Allow ID" on the next page
- "Block Diskspace Command" on page 402
- "Elevate LS" on page 403

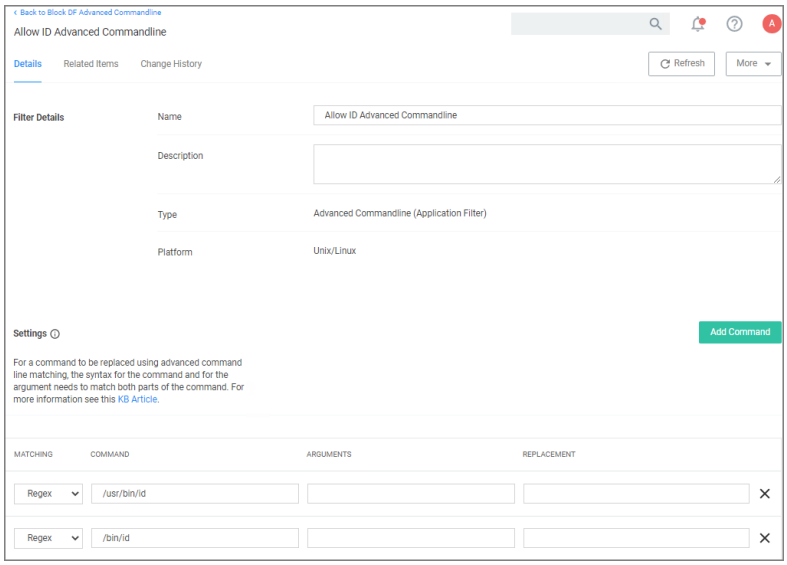
Wizard Flow Diagram

The following diagram shows the typical decision flow when using the policy wizard for creating Unix/Linux policies.

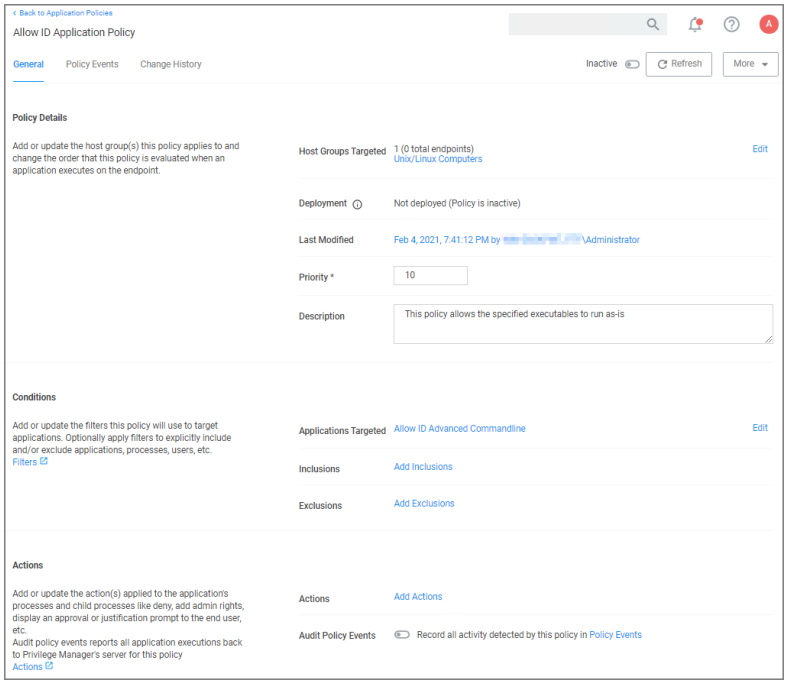


Allow ID

1. Navigate to your Unix/Linux computer group and select Application Policies.
2. Click **Create Policy**.
3. Using the Policy Wizard, create a controlling policy, click **Next Step**.
4. Select **Allow**, click **Next Step**.
5. Select **Executables**, click **Next Step**.
6. Select **Existing Filter**, search for select the **ID Advanded Commandline Filter**. If it doesn't exist, create it.



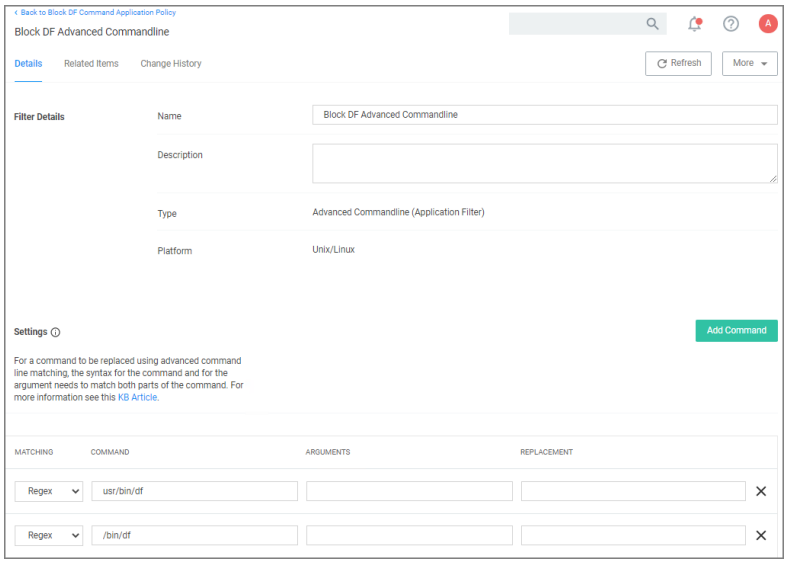
7. Click **Update**.
8. Click **Next Step**.
9. Name your policy, add a description.
10. Click **Create Policy**.



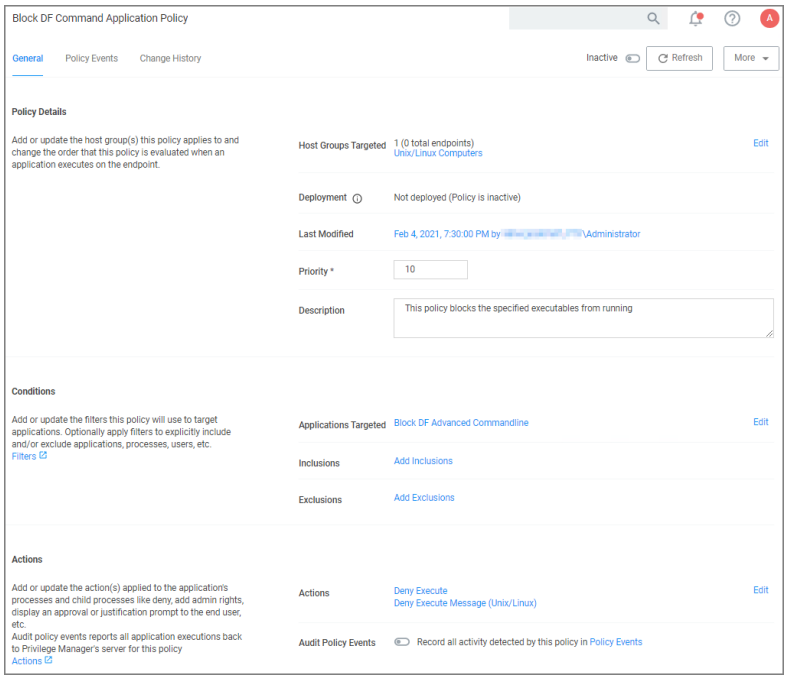
11. Set the **Inactive** switch to **Active**.
12. Next to **Deployment** click the **i** icon and run the **Resource and Collection Targeting Update** task.

Block Diskspace Command

1. Navigate to your Unix/Linux computer group and select Application Policies.
2. Click **Create Policy**.
3. Using the Policy Wizard, create a controlling policy, click **Next Step**.
4. Select **Block**, click **Next Step**.
5. Select **Executables**, click **Next Step**.
6. Select **Existing Filter**, search for select the **Block DF Advanded Commandline Filter**. If it doesn't exist, create it.



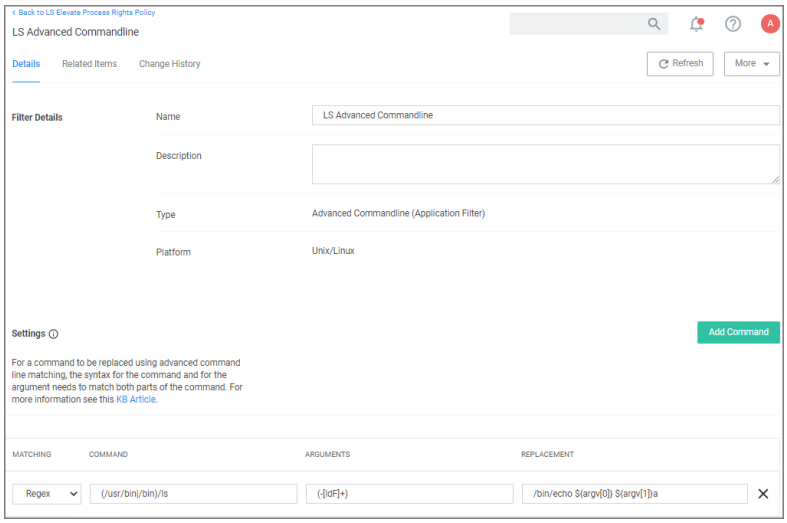
7. Click **Update**.
8. Click **Next Step**.
9. Name your policy, add a description.
10. Click **Create Policy**.



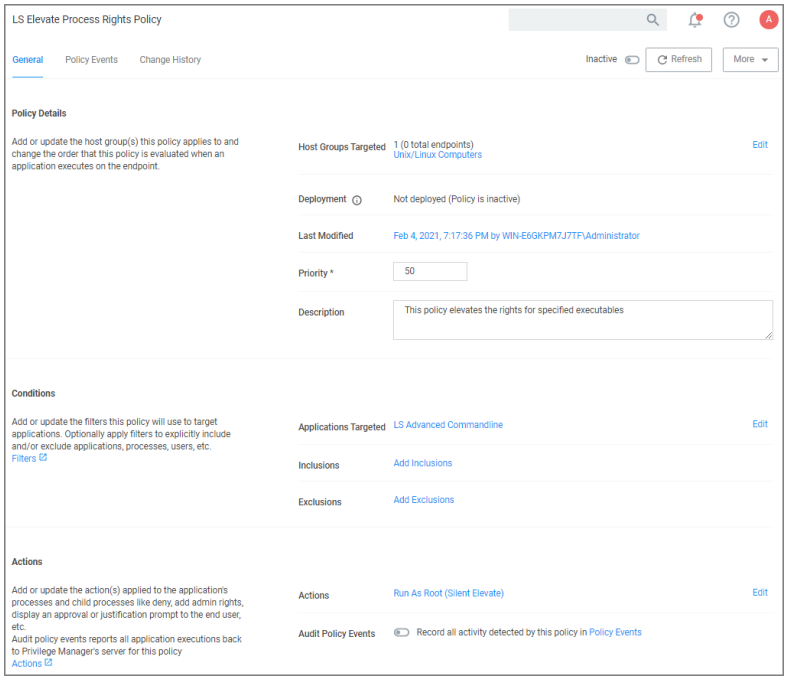
11. Set the **Inactive** switch to **Active**.
12. Next to **Deployment** click the **i** icon and run the **Resource and Collection Targeting Update** task.

Elevate LS

1. Navigate to your Unix/Linux computer group and select Application Policies.
2. Click **Create Policy**.
3. Using the Policy Wizard, create a controlling policy, click **Next Step**.
4. Select **Elevate**, click **Next Step**.
5. Select **Run Silently**, click **Next Step**.
6. Select **Executables**, click **Next Step**.
7. Select **Existing Filter**, search for select the **LS Advanded Commandline Filter**. If it doesn't exist, create it.



8. Click **Update**.
9. Click **Next Step**.
10. Name your policy, add a description.
11. Click **Create Policy**.



12. Set the **Inactive** switch to **Active**.
13. Next to **Deployment** click the **i** icon and run the **Resource and Collection Targeting Update** task.

Windows Policy Wizard

This section contains Windows policy wizard decision flow diagrams for controlling policies.

The following diagrams are available:

- "Creating a Controlling Elevation Policy for Windows" on page 419
- "Creating a Controlling Allow Policy for Windows" on page 416
- "Creating a Controlling Block Policy for Windows" on page 417
- "Creating a Controlling Restrict Policy for Windows" on page 420

Run as an Adminstrator

This topic describes the Privilege Manager**Right-Click Run As Thycotic Administrator**, or **Request Run As Administrator** (RRAA), functionality and cover use cases.

Note: Also refer to the Adjust Process Rights Action topic for further details and best practices.

RRAA Use Cases

Removing all accounts from the local Administrators Group creates several “Gotcha” situations:

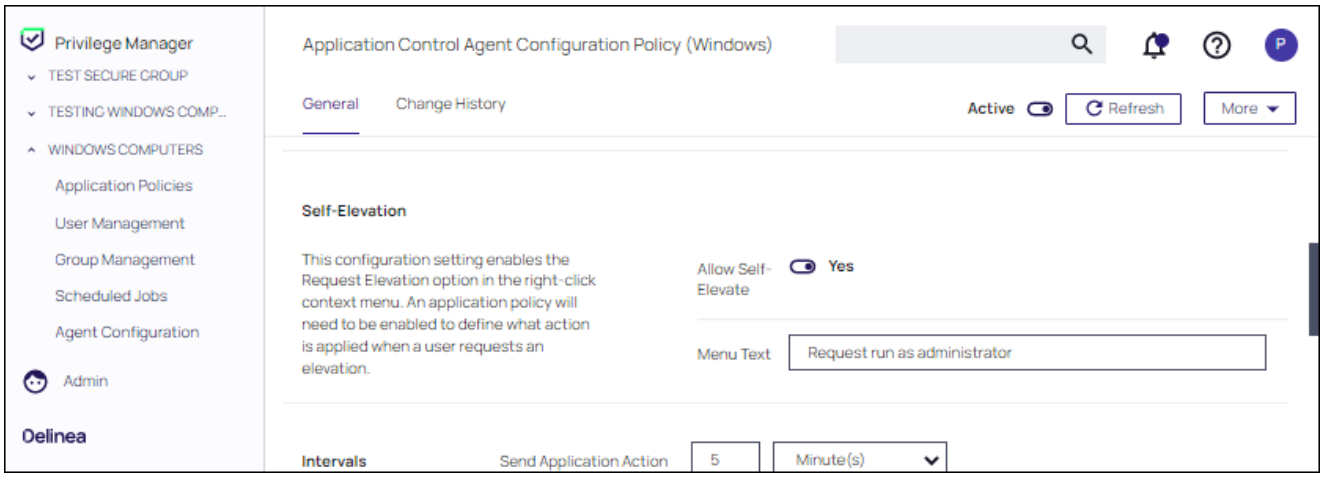
- The UAC prompt to Elevate becomes an un-answerable request when there are no account credentials to satisfy UAC with
- Trying to use the built-in Right Click "Run as Administrator" we also have no credentials that can be entered.

RRAA becomes a very useful support tool and can provide those “special” users unfettered access to admin functionality they demand.

RRAA is a tool that satisfies Admin removal issues when: you are under the gun of a deadline to remove Admin, in a very fast paced environment and understaffed to keep-up with policy creation, it can also provide the support staff with the super powers they need.

Background of RRAA

This function is built into the Privilege Manager Agent. There are different versions of the Agent and new versions sometimes have additional RRAA functionality, like the recent addition of .MSI file types to the right click option. This feature is for Windows Operating Systems only. It is toggled on or off via any of your **Windows Computer Groups | Agent Configuration** and under **Self-Elevation** set the switch to on.



Testing RRAA Policies

This section explains how to create a RRAA Elevation Policy for Developers. As described here, this feature will be added to all endpoints with the Application Control Agent. It will require authentication from a Developer to proceed, so other users won't be able to *use* the feature, but it will be present.

There are two steps to configuring the **Right-Click Run As Thycotic Administrator** feature.

One is the global configuration setting to enable the feature. Enabling this adds the “Request run as Thycotic Administrator” option to all endpoints with the Application Control Agent installed.

After enabling the global feature, Policies are created that assign Actions to this feature, typically based on specific use cases (such as the Developer use case detailed below).

If testing this feature in an environment with Agents deployed to production machines, consider first creating a Policy that targets all endpoints and all users that includes a custom Application Denied Message Action or Application Warning Message Action explaining that this feature isn't currently enabled, but may be used in the future by Helpdesk or other users. Then create a separate policy that has Resource Targets only for your test machines and a Policy Priority to occur earlier in processing. That way, your tests will be separate from the global actions of this feature.

Create a RRAA Elevation Policy for Developers

After the Right-Click Run As Thycotic Administrator feature is enabled, an Elevation Policy that handles the Elevation workflow will need to be created. The policy in this topic uses the default Resource Targets for All Windows computers with the Privilege Manager Agent installed. Using computer groups, smaller Resource Targets can be used and many custom options can be created to address many use cases in the environment, each having a customized Menu Text and resource specific targeting.

In the following example, a RRAA Elevation Policy will be created for the Developers group. First, a custom Message Action will be created to use on the Policy.

Advanced Message Actions

There are several Advanced Message Actions that can be displayed to end users. Advanced Message Actions can either require feedback in a justification and/or group member authentication, require approval from within Privilege

Manager when the process runs, or require no input.

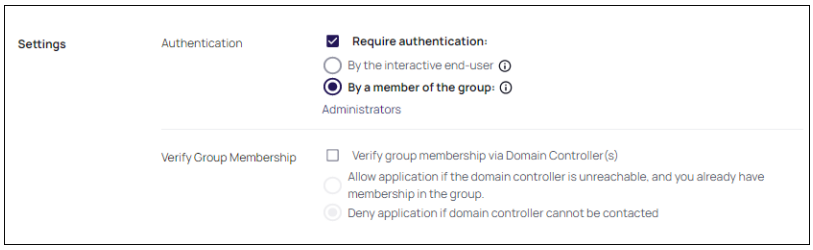
The most common Message Actions used with RRAA Policies are the Advanced Feedback Message Actions, including:

- Group Member Authenticated Message Action: This action will display a customized message to the user and requires authentication by a member of the specified group if the end-user is not a member.
- Authenticated Justification Message Action: This action will display an authentication prompt to the user before continuing to the process controlled by a policy.
- Justify Application Elevation Action: This action will display a justification prompt to the user before continuing to the process controlled by a policy.

Each of these Actions provide fields that can adjust the communication presented to the User.

As the following steps demonstrate, the Message Actions have several radio buttons in the Settings area to shape what they do and how they interact with the user.

These Actions are really just different radio button selections of two basic Actions. One Action with a Justification and the other Action without Justification.

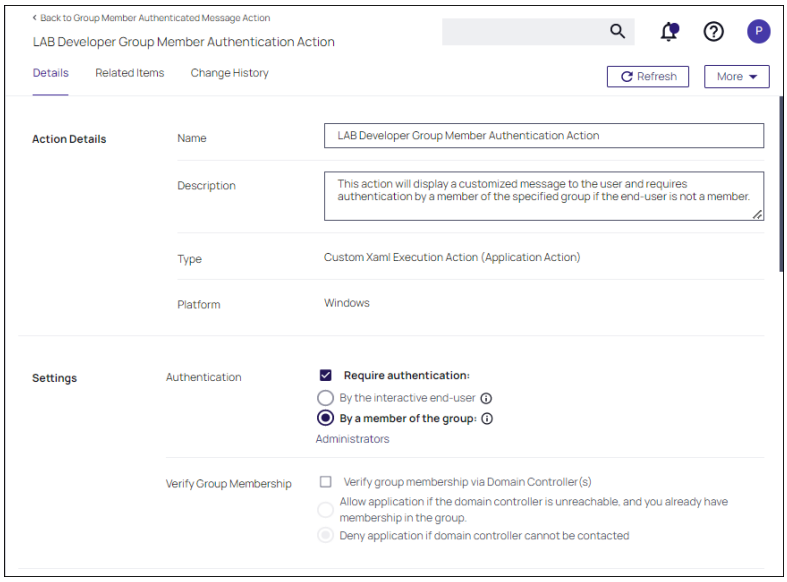


Custom Group Member Authentication Action for Developers

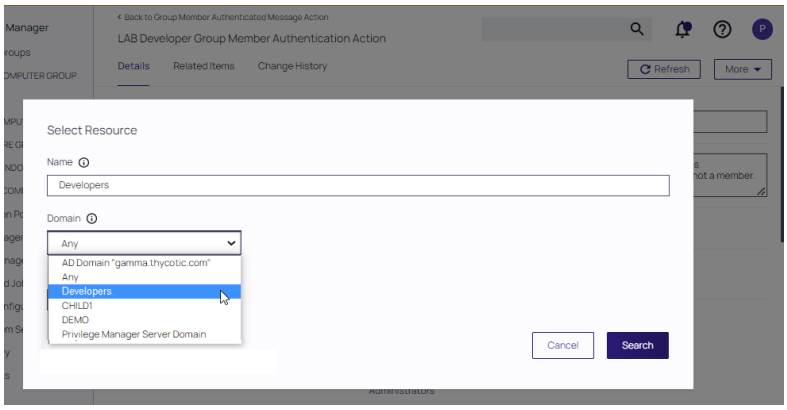
For this example, we will be using the “Group Member Authenticated Message Action” with the default radio button configuration. The Action will require credentials from a user who is a member of a specific AD group. This Action will not require justification.

To begin, find an existing Message Action to duplicate.

1. Navigate to **Admin | Actions**.
2. Search for **Group Member Authenticated Message Action**.
3. Click **Duplicate**.
4. In the **Duplicate** modal, enter the name *LAB Developer Group Member Authentication Action*.
5. Click **Create**.



6. Under Settings and **By a member of group**, click **Administrators**. As a resource select the AD group for your developers, in this example *Developers*. (Use **Search** to search and identify a resource.) Click **Save Changes**.

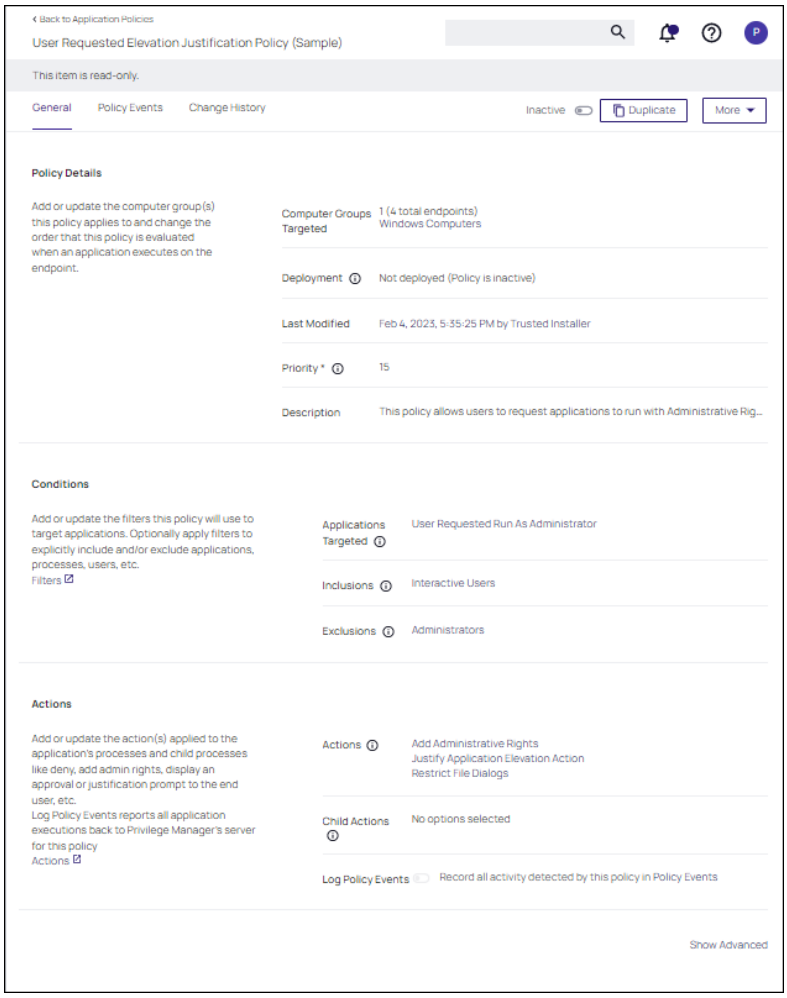


Custom RRAA Elevation Policy for Developers

To build the custom RRAA Elevation Policy for Developers, copy an existing RRAA Elevation Policy. A default policy is included with Privilege Manager.

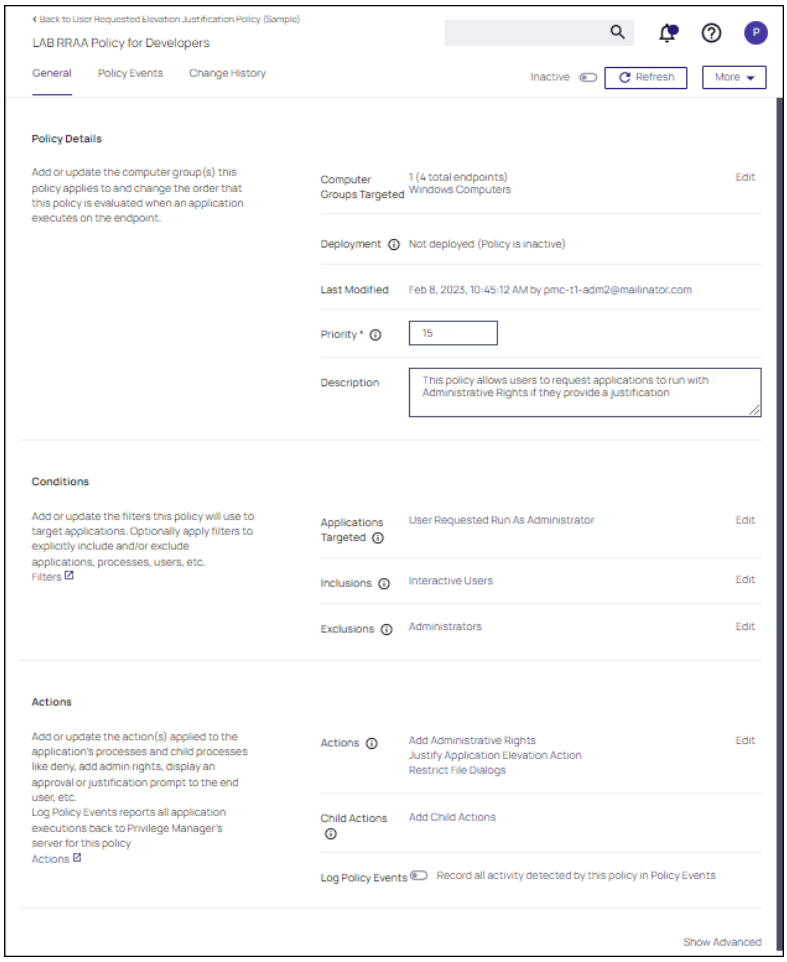
1. Navigate to your Windows Computer group.
2. Search for **User Requested Elevation Justification Policy (Sample)**, to locate the default policy.

Computer Groups



3. Click **Duplicate**. In the **Duplicate** modal, enter the name *LAB RRAA Policy for Developers*. Click **Create**.

Computer Groups

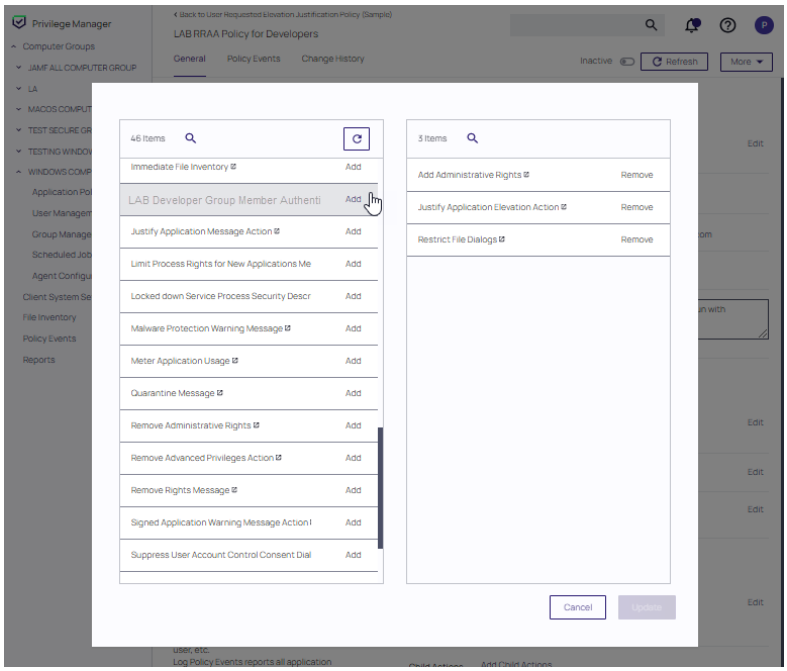


Under **Conditions** the policy includes the Application Target of **User Requested Run As Administrator**. This corresponds to the **Right-Click Run As Thycotic Administrator** option on the endpoint.

Under **Actions** the policy includes by default:

- Add Administrative Rights
- Justify Application Elevation Action
- Restrict File Dialogs

4. Next to these actions, click **Edit**.
   - Remove the **Justify Application Elevation Action** and **Restrict File Dialogs** default actions.
   - Search for and add the **LAB Developer Group Member Authentication Action**.
   - Click **Update**.



5. Click **Save Changes**.

With the **LAB RRAA Policy for Developers**, logged-on members of the Developers group can seamlessly get Admin rights when using the Right-Click Request Run As Thycotic Administrator.

Activate this policy, when you are ready to begin using it on endpoints.

Multiple RRAA Policies in the Same Policy Stack

Another common use case for the Right-Click Run As Thycotic Administrator feature is a RRAA Elevation Policy for Helpdesk. To do this, follow the same steps for the RRAA Elevation Policy for Developers, outlined above, using Helpdesk AD groups and naming conventions for the Action and Policy during creation.

It's possible to have multiple RRAA policies that work for different groups in the same Policy stack. To get this working, User Context Filters will be built in Privilege Manager that match the targeted AD groups.

Once the basic policies needed are made, and the User Context Filters are created, use the “Add Inclusion Filter” and “Add Exclusion Filter” sections under the Policy's “Conditions” to logically get all Policies working in your policy stack.

In the Developers & Helpdesk example:

- If the Current User on an endpoint is in the Developers AD group and initiates the Right-Click Run As Thycotic Administrator feature, the LAB Developer Group Member Authentication Action will execute, requiring the credentials of a member of the Developer AD group.
- A separate Policy is created that excludes the Developers User Context Filter (therefore, applies to all other users) and includes a custom Helpdesk Action that requires credentials from a member of a Helpdesk AD group and a justification/reason.

- If the Current User on an endpoint is not a member of the Developers AD group and initiates the Right-Click Run As Thycotic Administrator feature, the custom Helpdesk Action executes.
- The Helpdesk's RRAA Policy would not work when the computer User is in the Developers group, but the Helpdesk policy would work on all other computers regardless of who the User is.

This example gives Helpdesk users a workflow to enter their credentials on any computer to request elevation for supporting all computers not having a separate RRAA Policy of their own (in the above example, only the Developers have a separate RRAA Policy).

Other examples can be added for other use cases. By utilizing user AD groups, this can be managed in AD with corresponding User Context Filters created in Privilege Manager and assigned to Policies.

If more than two RRAA policies are required like adding with and without Justifications, sorting the Inclusion/Exclusion logic would be required. The Global RRAA has all other RRAA group filters in the Exclusions, the user specific RRAA get only their Group filter put in the Inclusions.

If the Inclusion/Exclusion logic is managed correctly, the RRAA Policies could use the same Policy Priority, but Policy Priorities can also help with the logic. Assume the RRAA Elevation Policy for Developers has a Policy Priority of 14, and the RRAA Elevation Policy for Helpdesk has a Policy Priority of 15. In this example, the RRAA Elevation Policy for Developers has priority over the RRAA Elevation Policy for Helpdesk.

Also, the Policy Priority of the RRAA Elevation Policies matters in relation to the other Policies in the Policy stack. Other Policies with Policy Priorities to occur before the RRAA Elevation Policies – such as Deny Policies – would happen before the RRAA Elevation. This is why the single, default User Requested Elevation Justification Policy has a Policy Priority of 15, to occur early in the Policy stack.

Note: Enabling the right-rlick **Run As Thycotic Administrator** feature via **Computer Groups** | **Agent Configuration** will add the right-click **Run As Thycotic Administrator** feature to all machines with the Application Control Agent installed.

If not using the RRAA Elevation Policy for Helpdesk example for all other RRAA use cases not defined, consider a Global RRAA Policy that adds a Notification Message Action to inform these users that they do not have permissions to run the right-click **Run As Thycotic Administrator** feature.

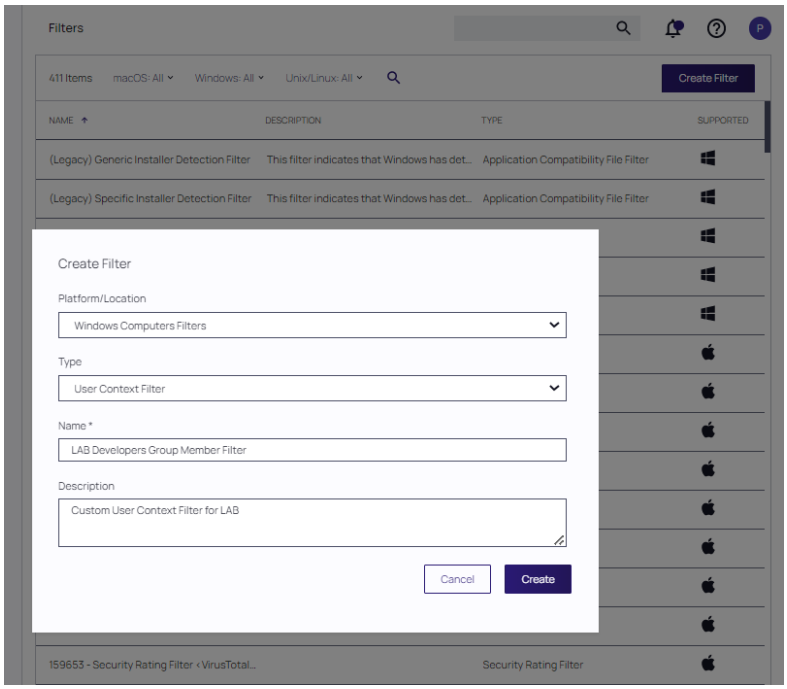
User Context Filter for Developers

A User Context Filter can be created for the Developers AD group. That filter can then be used as an Inclusion Filter on the RRAA Elevation Policy for Developers.

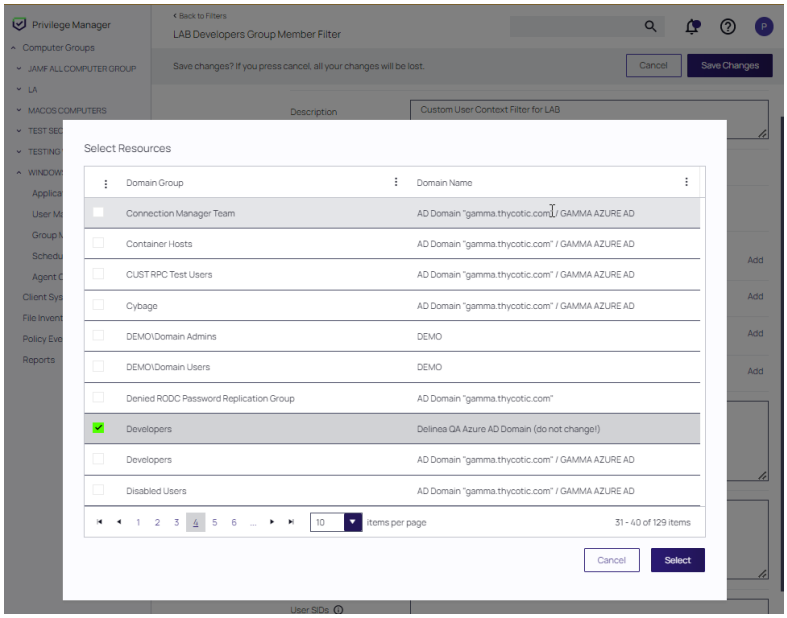
In the use case of a separate RRAA Elevation Policy for Helpdesk, the User Context Filter for the Developers AD group will also be used as an Exclusion Filter on the RRAA Elevation Policy for Helpdesk.

Create a Custom User Context Filter for Developers

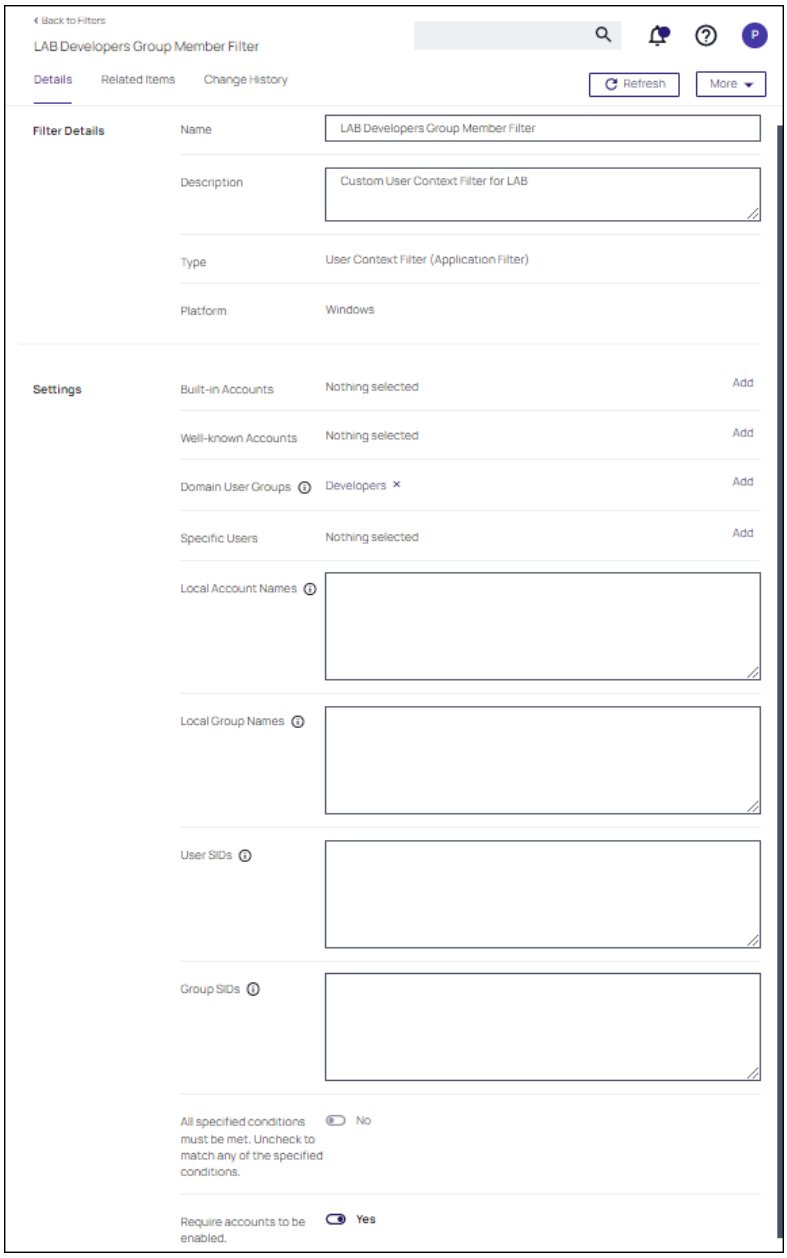
1. Navigate to Admin | Filters and click **Create Filter**.
2. From the **Platform** drop-down, select **Windows Computers Filters**.
3. From the **Type** drop-down, select **User Context Filter** and enter the name *LAB Developers Group Member Filter*. Click **Create**.



4. Under **Settings** next to **Domain User Groups**, click **Add**. In the **Select Resources** modal, click **Search** and add the **Developers** AD group. Click **Select**.



5. Set the **Require accounts to be enabled** switch to **Yes**.
6. Click **Save Changes**.

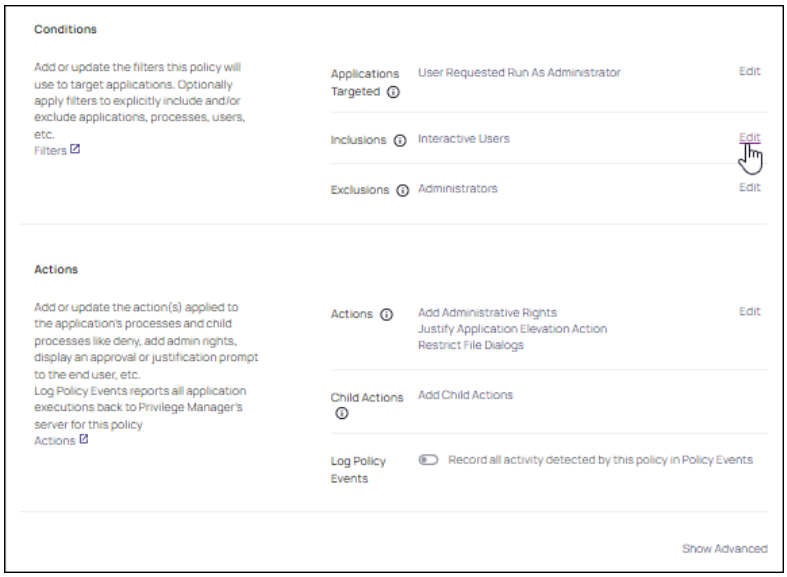


Include User Context Filter for Developers to RRAA Elevation Policies for Developers

Adding **LAB Developers Group Member Filter** to the **RRAA Elevation Policy for Developers** will result in the Actions on this policy only executing if a member of the Developers AD group initiates the right-click **Run As Thycotic Administrator**.

1. Navigate to your **LAB RRAA Policy for Developers** policy.
2. Under **Conditions** next to **Inclusions**, click **Edit**.
3. Search for and add the **LAB Developers Group Member Filter**, you might have to refresh the available filter list.

4. Click **Update**.
5. Click **Save Changes**.



Exclude User Context Filter for Developers to RRAA Elevation Policies for Helpdesk

If an **RRAA Elevation Policy for Helpdesk** was created, as described in the "Multiple RRAA Policies in the Same Policy Stack" section of this document, the **LAB Developers Group Member** filter can be added to the **RRAA Elevation Policy for Helpdesk** as an Exclusion filter to ensure that there is not a conflict between which action to run when Developers initiate the right-click **Run As Thycotic Administrator** feature.

To create an **RRAA Elevation Policy for Helpdesk**, follow the same steps for the **RRAA Elevation Policy for Developers**, as described in this document, but use the Helpdesk AD group(s) and naming conventions for the action and policy.

A RRAA Elevation Policy for Helpdesk may require or desire different types of Message Actions than used on the RRAA Elevation Policy for Developers. Consider using the Authenticated Justification Message Action for the RRAA Elevation Policy for Helpdesk.

To add the **LAB Developers Group Member** filter as an Exclusion filter:

1. Navigate to your **LAB RRAA Policy for Helpdesk** policy.
2. Under **Conditions** next to **Exclusions**, click **Edit**.
3. Search for and add the **LAB Developers Group Member Filter**, you might have to refresh the available filter list. Click **Update**.
4. Click **Save Changes**.

The Helpdesk policy is now finished. When ready to use, click **Enable** on the **General** tab and click **Save**.

Windows Policy Wizard

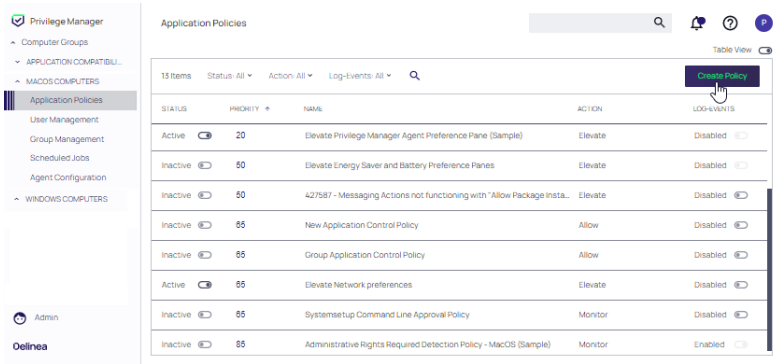
This section contains Windows policy wizard decision flow diagrams for controlling policies.

The following diagrams are available:

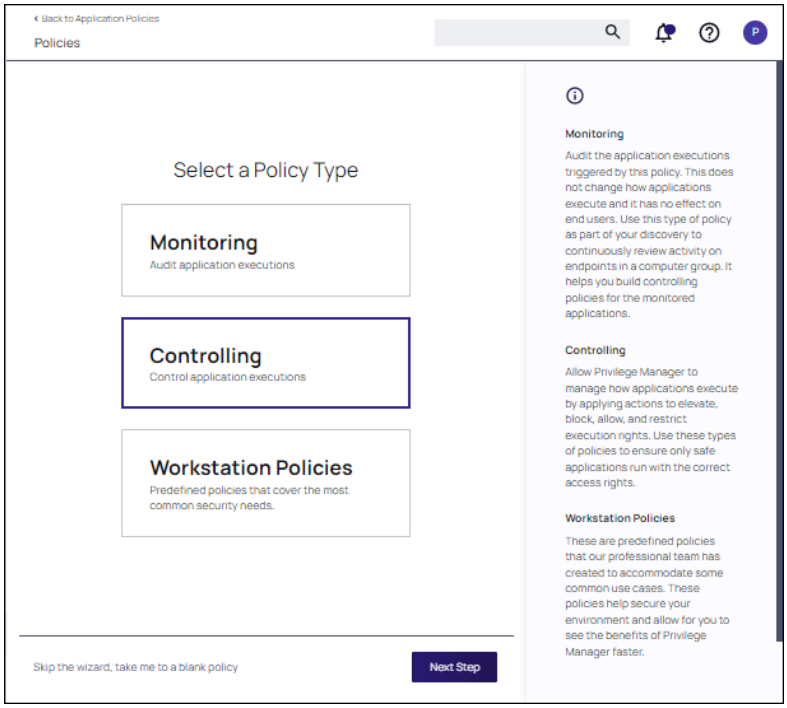
- "Creating a Controlling Elevation Policy for Windows" on page 419
- "Creating a Controlling Allow Policy for Windows" below
- "Creating a Controlling Block Policy for Windows" on the next page
- "Creating a Controlling Restrict Policy for Windows" on page 420

Creating a Controlling Allow Policy for Windows

1. For any of your Computer Groups navigate to **Application Policies**.

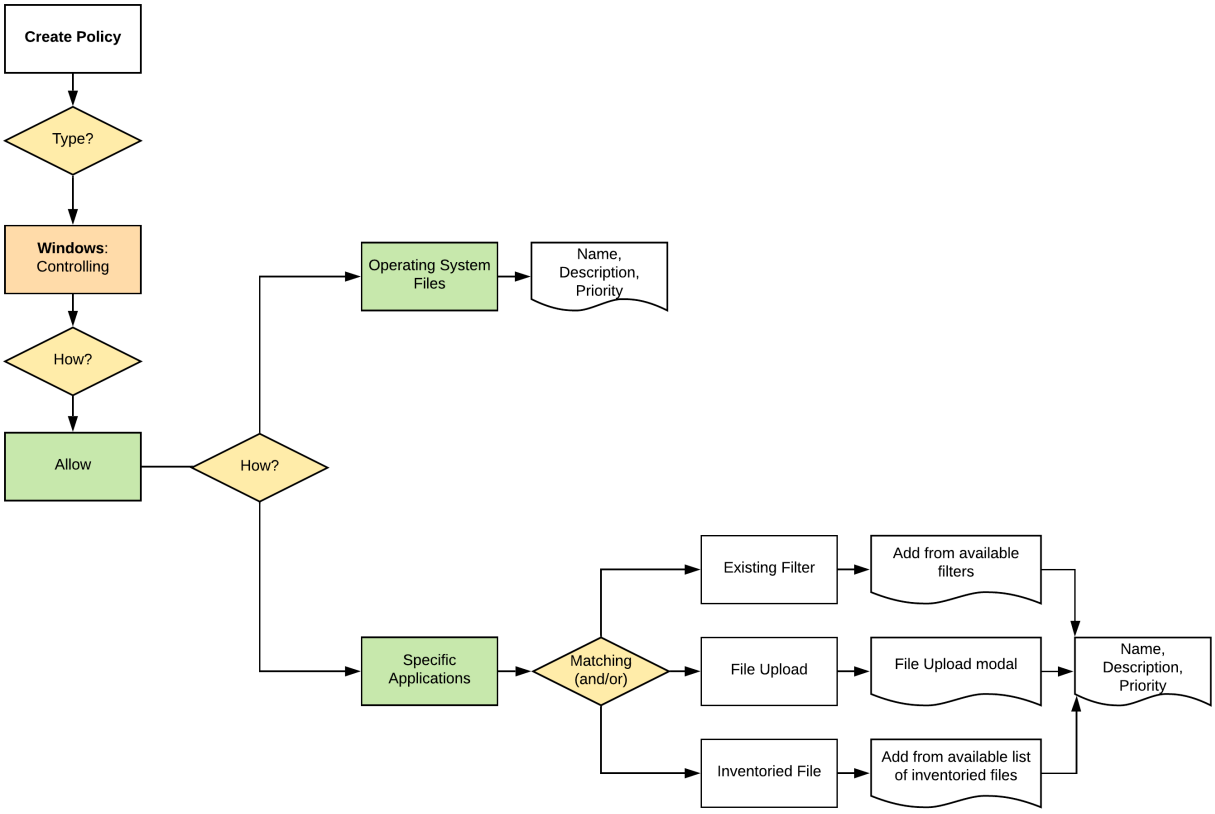


2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:



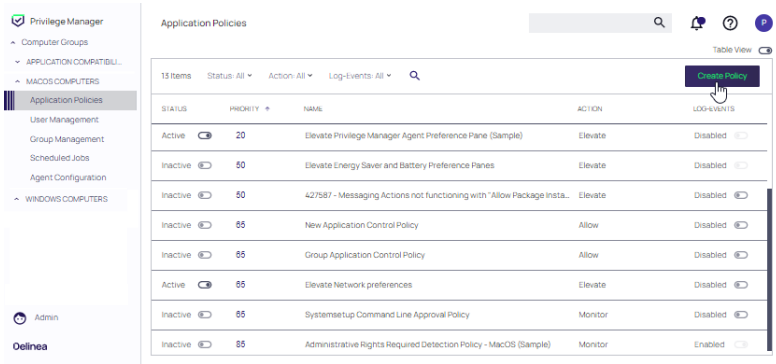
3. After assigning a name, description and verifying the priority number, click **Create Policy**.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

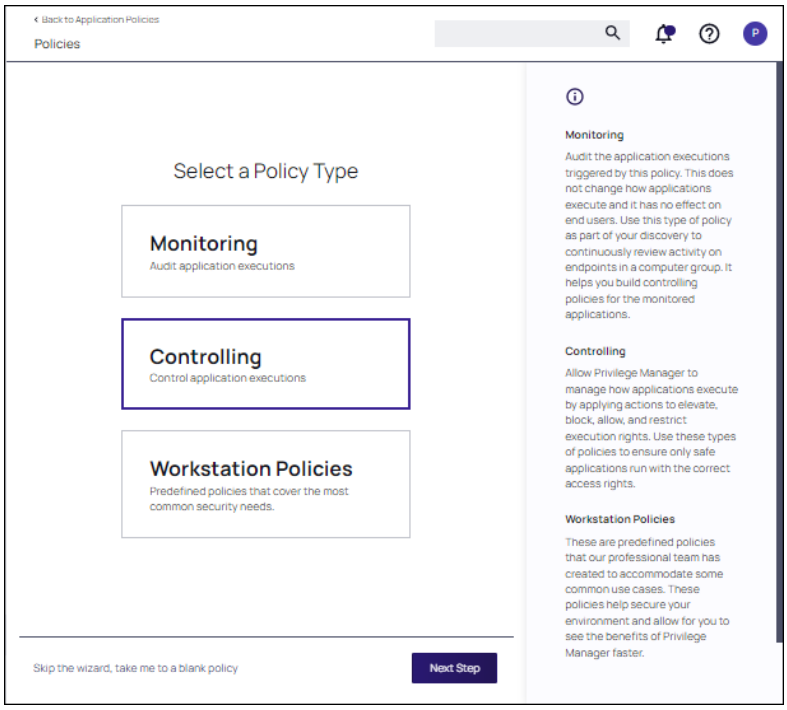
The wizard provides on page help explaining the different options available to the user.

Creating a Controlling Block Policy for Windows

1. For any of your Computer Groups navigate to **Application Policies**.

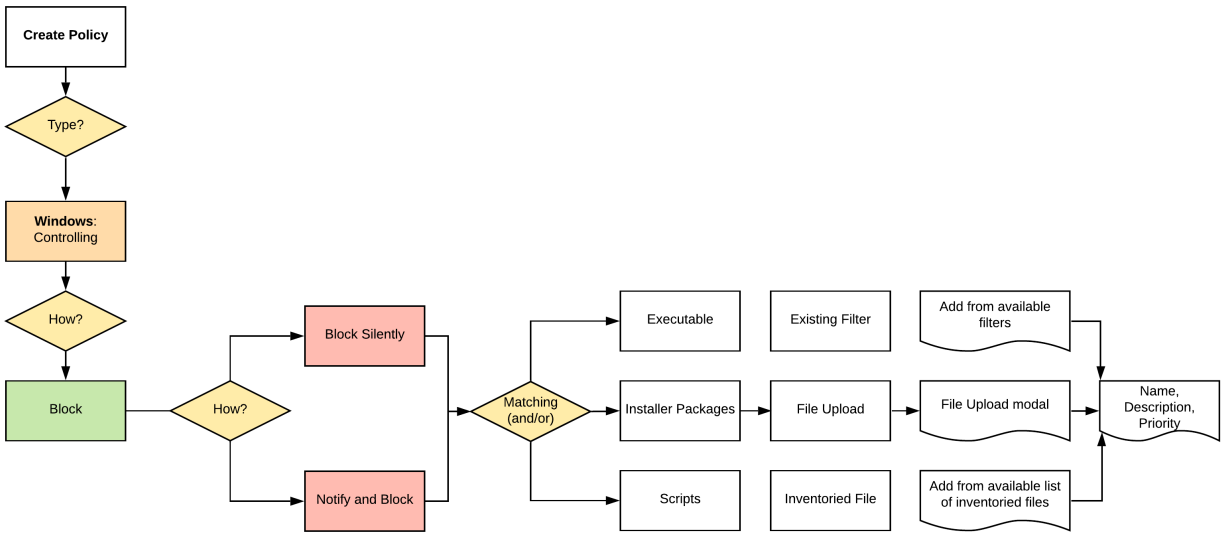


2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:



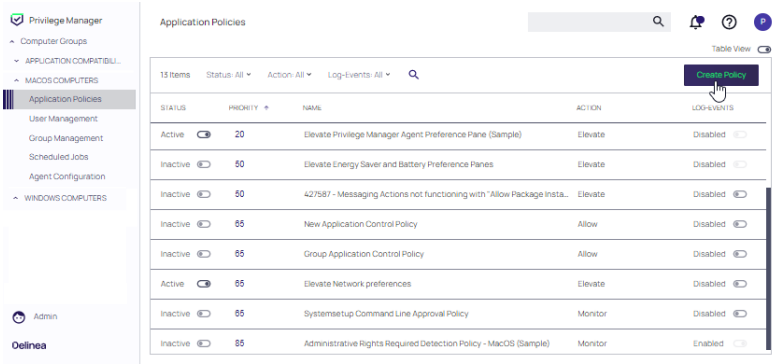
3. After assigning a name, description and verifying the priority number, click **Create Policy**.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

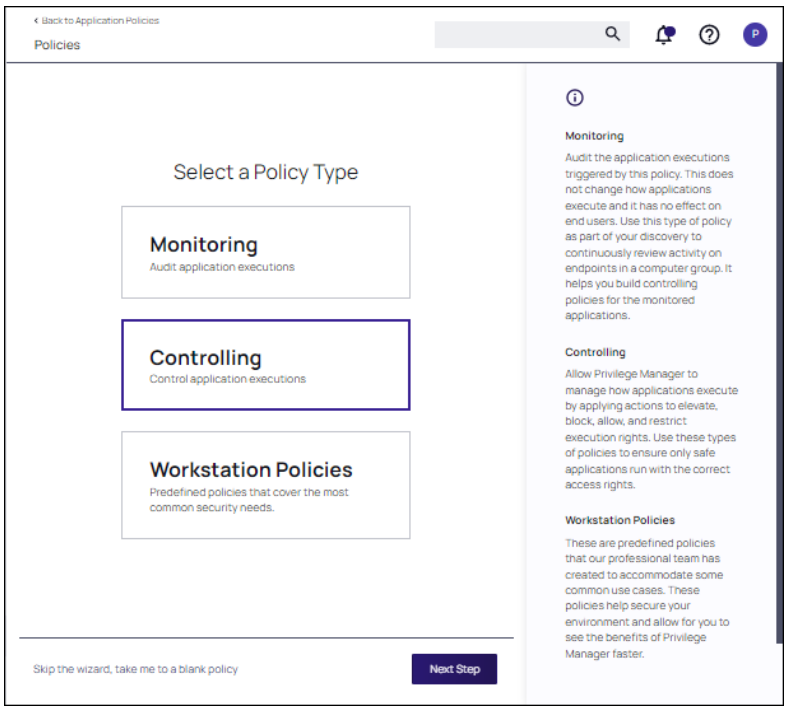
The wizard provides on page help explaining the different options available to the user.

Creating a Controlling Elevation Policy for Windows

1. For any of your Computer Groups navigate to **Application Policies**.

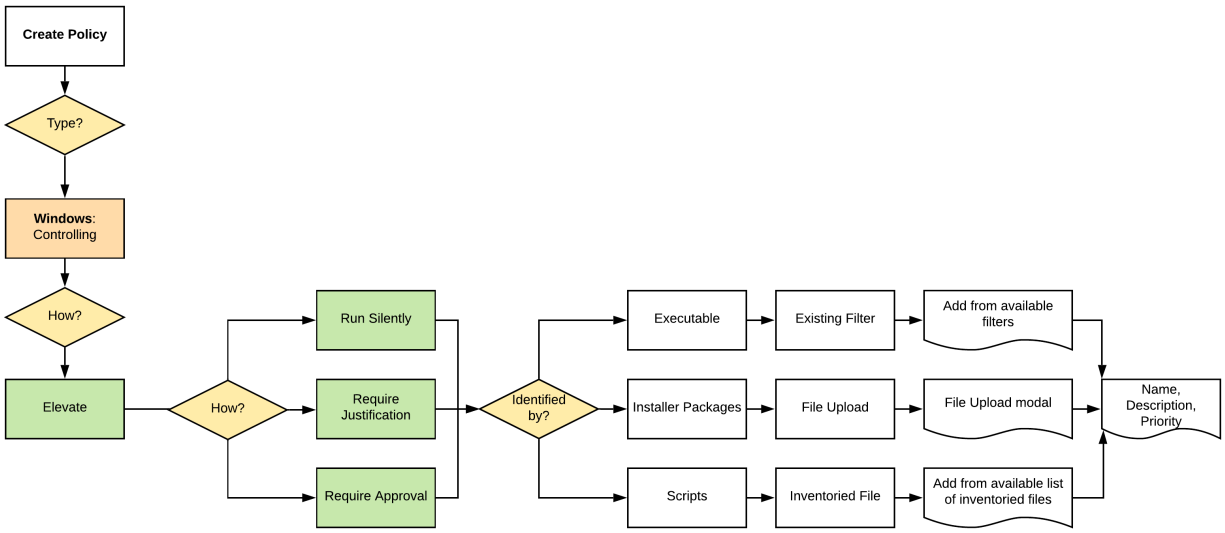


2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:



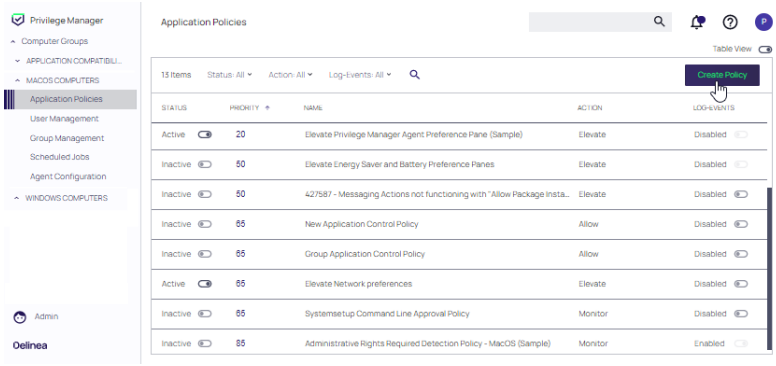
3. After assigning a name, description and verifying the priority number, click **Create Policy**.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

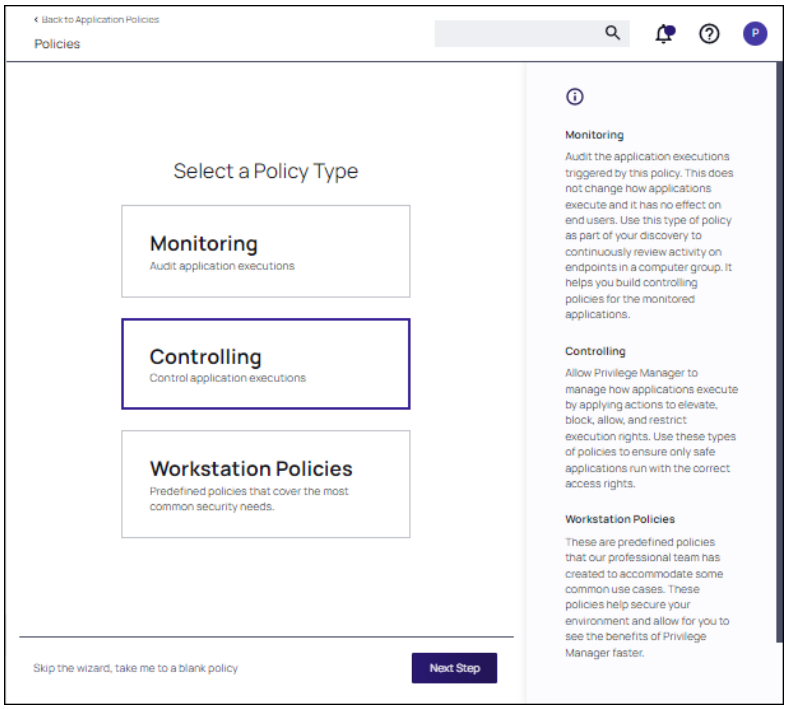
The wizard provides on page help explaining the different options available to the user.

Creating a Controlling Restrict Policy for Windows

1. For any of your Computer Groups navigate to **Application Policies**.

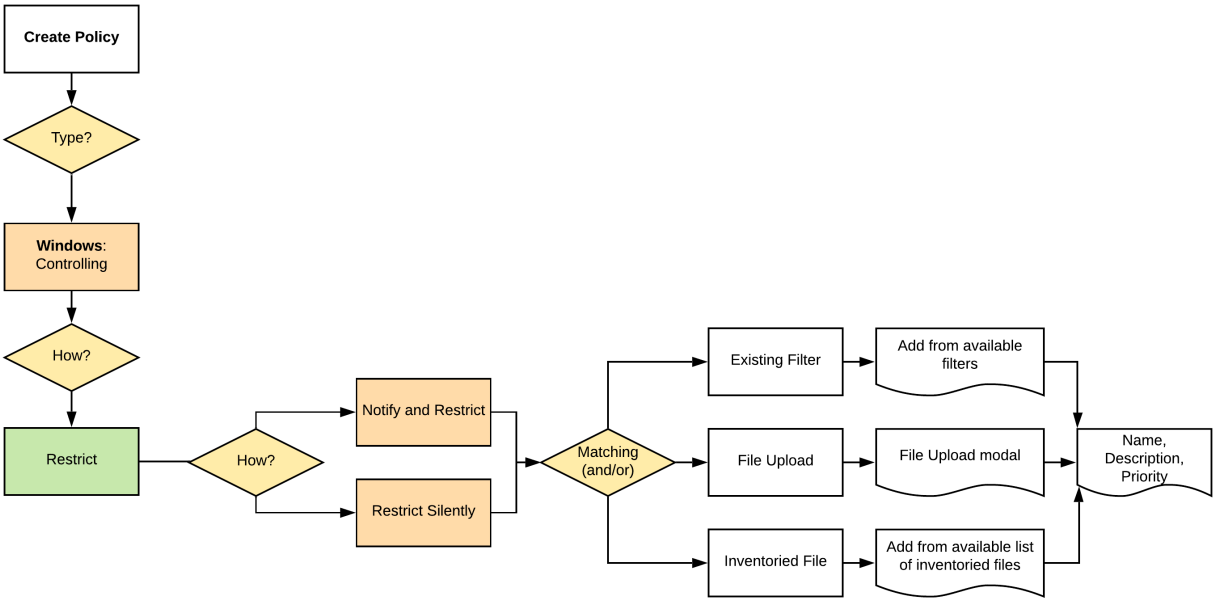


2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:



3. After assigning a name, description and verifying the priority number, click **Create Policy**.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

The wizard provides on page help explaining the different options available to the user.

Delinea Policy Framework (DPF)

This topic outlines a legacy policy set and deployment methodology for Delinea Privilege Manager.

> **Note:** With Privilege Manager version 11.4.1, an updated set of Workstation policies were developed for use in the "Policy Wizard" on page 250, that takes a stepped approach to defining and implementing policy sets. Delinea recommends the use of these Workstation policies going forward. Workstation policies are also referenced along with the predefined Computer Groups in the privilege-manager Tutorial.

Approach

The biggest risk when implementing Endpoint Privilege Management (EPM) solutions like Delinea Privilege Manager is impacting user productivity. This approach has several key aims, which are highlighted below:

- Take the best practices learned from thousands of successful implementations and make them available to all customers.
- Provide reduced time to value, with a policy set that can be enabled in seconds.
- Simplify and reduce the overhead of day-to-day management of endpoint privilege and application management.

As an example, where a user's admin rights are removed on a Monday and they come into work on a Tuesday to discover that applications they need to run to perform their core job function cannot run or are missing functionality without administrative privileges. This approach mitigates that risk by ensuring that during the initial stages of a deployment users are provided with flexible 'on demand' elevation to run applications with elevated privileges where required.

This means that admin rights can be removed without the need for lengthy discovery phases meaning customers get more value from the solution from the point of implementation.

One Size Does Not Fit All

Different users and communities of users require very different application sets and privilege levels in their endpoint environment. The Delinea policy approach allows customers to define users or groups of users into a high, medium, or low privilege filter based on Active Directory group membership or by targeting individual users. A high-level summary of the out of the box user experience is provided below.

- **High Privilege**: Provides users with a 'Pseudo Admin' experience, any application can be elevated on demand by right-clicking and selecting run as administrator. This policy set is typically aimed at the most technical users such as Developers and IT administrators.
- **Medium Privilege**: Provides users with a highly flexible experience where most applications can be elevated on-demand. High risk applications such as scripting engines require approval for elevated execution. This policy set is typically aimed at technical users.
- **Low Privilege**: Provides a highly secure application environment where users are unable to run any application with elevation without approval. This policy set is typically aimed at non-technical users who do not regularly need to install new applications.

The out-of-the-box user experience can be changed in a few clicks by replacing messaging. Customizable messages can be used to change the effective privilege levels at any point from a warning message to a justification or approval workflow.

Application Control

The approach also utilizes an intelligent approach to application allow-listing that leverages the core security concept of trusted file ownership.

Applications with trusted ownership (owned by Local System, Trusted Installer, Administrators by default) that are commonly found in the enterprise environment, will be allowed to execute out of the box. Applications that don't match against the allow list will hit a catch-all policy. The catch-all policy starts with a 'soft' audit approach, which allows customers to monitor unknown applications and refine allow listing before hardening the catch-all to an appropriate level for different user communities.

Policy Set Overview

The following section provides a high-level overview of the policies included in the TPF policy set.

Priority	Policy Name	Behavior Description
5	THY - Malware Protection Policy	Catches any unsigned and untrusted application that runs as a child process of high-risk applications such as Microsoft Office applications, email clients and browsers.
6	THY - LOLBAS Attack Protection	Protects vulnerable applications from being exploited using 'Living off the Land Binaries and Scripts' attack vectors.
11	THY - GLOBAL - Blocked Applications	Targets explicitly defined applications and denies execution with a visible message. All applications matching this policy are audited.
12	THY - GLOBAL: Silently Elevated Applications	This policy targets explicitly defined executable applications and elevates the application with no visible messaging.
13	THY - GLOBAL: Silently Elevated Installers	This policy targets explicitly defined Microsoft Installers and elevates silently.
14	THY - GLOBAL - Allow List (Explicit)	This policy targets explicitly defined applications that are approved for non-elevated execution.
21	THY - HIGH PRIVILEGE - Silently Elevated Applications	This policy targets explicitly defined executable applications for high privilege users and elevates the application with no visible messaging.

Priority	Policy Name	Behavior Description
22	THY - HIGH PRIVILEGE - Silently Elevated Installers	This policy targets explicitly defined Microsoft Installers for high privilege users and elevates the application with no visible messaging.
23	THY: HIGH PRIVILEGE: High Risk Applications	This policy targets a list of powerful, high risk applications. Users will be prompted for justification when elevating these applications. All applications matching this policy are audited.
24	THY - HIGH PRIVILEGE - High Risk Windows Settings	This policy targets high risk windows settings areas and presents a justification message which needs to be completed before execution is possible. All applications matching this policy are audited.
25	THY - HIGH PRIVILEGE - UAC Replacement (Signed Applications)	Targets any signed application that generates a User Account Control (UAC) dialogue. A warning message is displayed prior to elevated execution. All applications matching this policy are audited.
26	THY - HIGH PRIVILEGE - UAC replacement (Unsigned Applications)	Targets any unsigned application that generates a User Account Control (UAC) dialogue. A warning message is displayed prior to elevated execution. All applications matching this policy are audited.
27	THY - HIGH PRIVILEGE - Allow List (Trusted Owners)	This policy will allow applications with a trusted owner or that are explicitly defined to run with standard user rights, no messaging is displayed.
28	THY: HIGH PRIVILEGE - Catchall	This policy targets any application that has not matched against a previous policy for users defined within the High Privilege filter. This policy should not be enabled without High Privilege - Allow List also being enabled, doing so will generate large amounts of feedback data.
31	THY - MEDIUM PRIVILEGE - Silently Elevated Applications	This policy elevates targeted applications for users defined within the Medium Privilege Filter.

Priority	Policy Name	Behavior Description
32	THY - MEDIUM PRIVILEGE - Silently Elevated Installers	This policy elevates targeted installers for users defined within thee Medium Privilege filter with no messaging displayed.
33	THY - MEDIUM PRIVILEGE - High Risk Applications	This policy targets high risk applications and presents an approval workflow prior to elevated execution.
34	THY - MEDIUM PRIVILEGE - High Risk Windows Settings	This policy targets high risk windows settings areas and presents an approval workflow prior to elevated execution. All applications matching this policy are audited.
35	THY - MEDIUM PRIVILEGE - UAC Replacement (Signed Applications)	Targets any signed application that generates a User Account Control (UAC) dialogue. A warning message is displayed prior to elevated execution. All applications matching this policy are audited.
36	THY - MEDIUM PRIVILEGE - UAC replacement (Unsigned Applications)	Targets any unsigned application that generates a User Account Control (UAC) dialogue. A warning message is displayed prior to elevated execution.
37	THY - MEDIUM PRIVILEGE - Allow List (Trusted Owners)	This policy will allow applications with a trusted owner or that are explicitly defined to run with standard user rights, no messaging is displayed.
38	THY - MEDIUM PRIVILEGE - Catchall	This policy targets any application that has not matched against a previous policy for users defined within the High Privilege filter. This policy should not be enabled without High Privilege - Allow List also being enabled, doing so will generate large amounts of feedback data.
41	THY - LOW PRIVILEGE - High Risk Applications	This policy targets high risk applications and presents an approval workflow prior to elevated execution.

Priority	Policy Name	Behavior Description
42	THY - LOW PRIVILEGE - High Risk Windows Settings	This policy targets high risk windows settings areas and presents an approval workflow prior to elevated execution. All applications matching this policy are audited.
43	THY - LOW PRIVILEGE - UAC Replacement (Signed Applications)	This policy targets any application that generates a UAC prompt and has a valid digital certificate. Elevated execution requires approval.
44	THY - LOW PRIVILEGE - UAC replacement (Unsigned Applications)	Targets any application that generates a UAC prompt and does not have a valid digital certificate. Elevated execution requires approval.
45	THY - LOW PRIVILEGE - Allow list (Trusted Owners)	Targets any application that is owned by a trusted owner or explicitly defined applications and allows non-elevated execution with no visible messaging.
46	THY - LOW PRIVILEGE - Catchall	Targets any application that has not been matched against a higher priority policy. This policy allows on-elevated execution with no visible messaging. All applications matching this policy are audited.

Deployment Steps

Download the latest version of the Thycotic Policy Framework (TPF) from the Config Feeds. Once installed, the policy set is available in the Thycotic Policy Framework folder, usually at `https://[yourprivilegemangerinstance]/TMS/PrivilegeManager/#/folders/all/dfa7db45-f75c-4e31-be53-6281b1d4ce39]`.

Initial Configuration Steps

In addition to installing the config feed with the policy set and following the general initial setup guidelines, the following configuration should be performed:

Set up Active Directory / Azure AD integration for administrative console access and policy targeting.

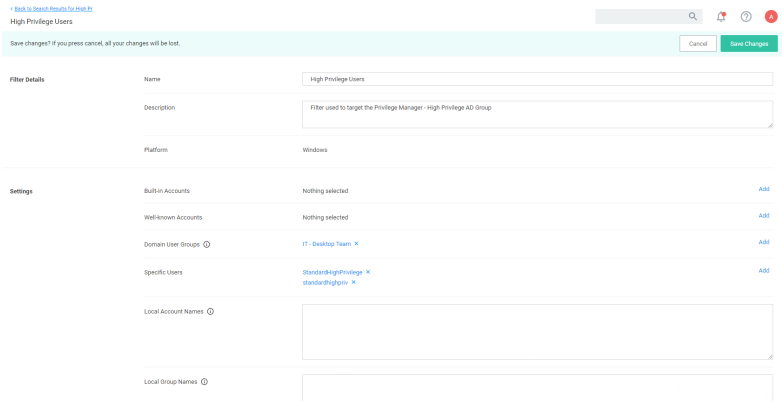
To allow users to authenticate with the Privilege Manager administrative console using their AD or Azure AD identity you should configure the AD or Azure AD integration. This can also be used to target TPF policies to specific users or security groups.

Build User Context Filters and or Resource Targets for Policy Targeting

Privilege Manager policies can be targeted at the user and or computer level. To target policies to specific users or security groups User Context filters can be created. The TPF set comes with three out of the box user context filters for High, Medium and Low Privilege Users.

Adding Users to High, Medium, or Low Privilege User Context Filters

1. In the Privilege Manager console search for **High Privilege Users** or select the **High Privilege Users filter** from any of the high privilege policies.
2. Search for and add local or domain users or Active Directory Security Groups to the filter:



3. Click **Save Changes**.

Privilege Manager also provides the ability to build resource targets, which are groups of computers that policies can target.

Policy Management and Refinement

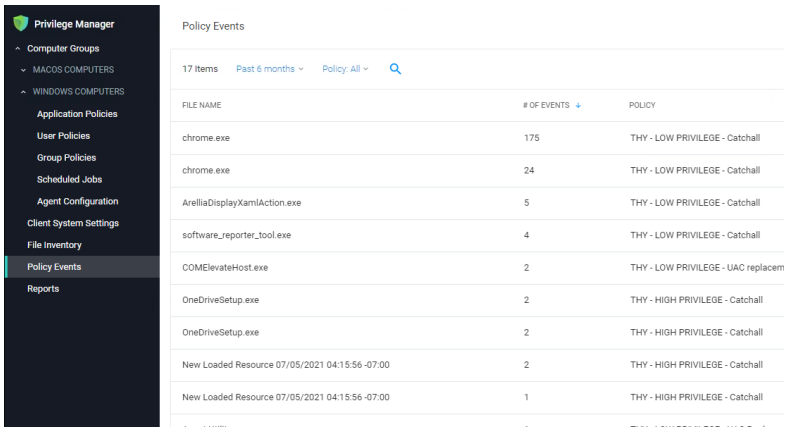
Before deploying any policies, you should add any known applications to relevant policies. For example, if you are aware of corporately approved applications that are used by all users which require admin rights, you can add application filters to the THY: GLOBAL: Allow List (Explicit) policy.

There are a number of ways application targets can be created:

- Manually by creating a blank win32 filter and targeting specific application metadata fields.
- By uploading an application file.
- Waiting for the TPF policies to generate application audit events and creating filters directly from the event.

Policy Refinement after Deployment

1. On a regular basis (as frequently as possible during the initial stages of the deployment) open the **Policy Events Report**:



2. From the left-hand menu, select **Policy Events**.
3. The report should default to sorting by the **# of events field**.
4. For each application in the list, review and decide how you want to handle the application. There are a number of options to consider:
   - Add to Global: Silently Elevated Applications or Installers to allow silent, elevated execution for **all users**.
   - Add to High/medium: Silently Elevated Applications or Installers to allow silent, elevated execution for users within the scope of the chosen policy.
   - Add to restricted applications to allow execution with approval workflow.
   - Do Nothing (User will continue to receive UAC replacement messaging, which will likely be hardened).
   - Add to Global: Block List.

     Note: The key consideration in making this decision, is the number of users executing the application and the number of times they are executing it. The higher these numbers the more impactful gating the application with an approval workflow would be.
5. Once number of new applications hitting UAC replacement plateaus, add more users to scope OR harden UAC replacement.
6. If application Control is required, review applications hitting catch-all, review and perform one of the following actions:
   a. Add to High/Medium/Low Allow List.
   b. Add to Global - Block List.
   c. Do nothing (Application will be gated with approval workflow when catch-all is hardened).
   d. Once number of unknown applications hitting the catch-all plateaus, add more users to scope AND/OR harden catch-all.

Frequently Asked Questions

Q1. Why is there no user context filter for low privileged Users?

A1: This is by design, as the Low Flexibility policy set does not have any user context inclusion filters. It will apply to any user that is not in the scope of the High or Medium Flexibility policies. Effectively, the Low Privilege policy set functions as a catch-all policy set and avoids the risk that user is not included in a filter and has no policies applied.

Q2. Why are there no Silent Elevation policies for low privilege users?

A2: It is highly unlikely that applications need to be elevated for low privilege users without being elevated for all users. Typically, any application requiring elevation for low privilege users can be targeted in the global elevation policies.

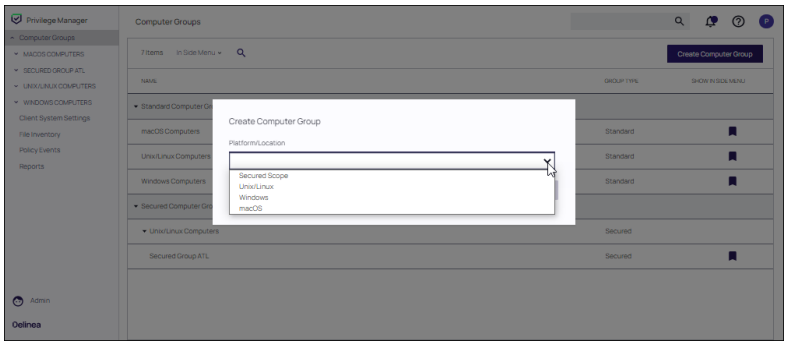
Q3. Why is the catch-all policy configured to allow unknown applications to run?

A3: Any policy set that attempted to block or gate unknown applications at the point of deployment would be highly disruptive to users and/or generate high volumes of approval requests to support teams. Catch-all policies are intended to quickly collect audit data that can be used to refine allow listing before being hardened.

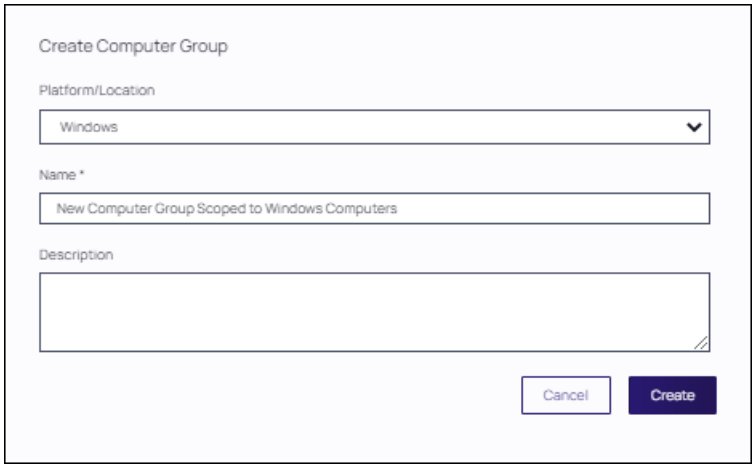
Creating Computer Groups

To add new Computer Groups for your organization's environment:

1. On the Compter Groups page, click **Create Computer Group**.
2. From the **Platform/Location** drop-down list box, select macOS, Secured Scope, Unix/Linux, or Windows.



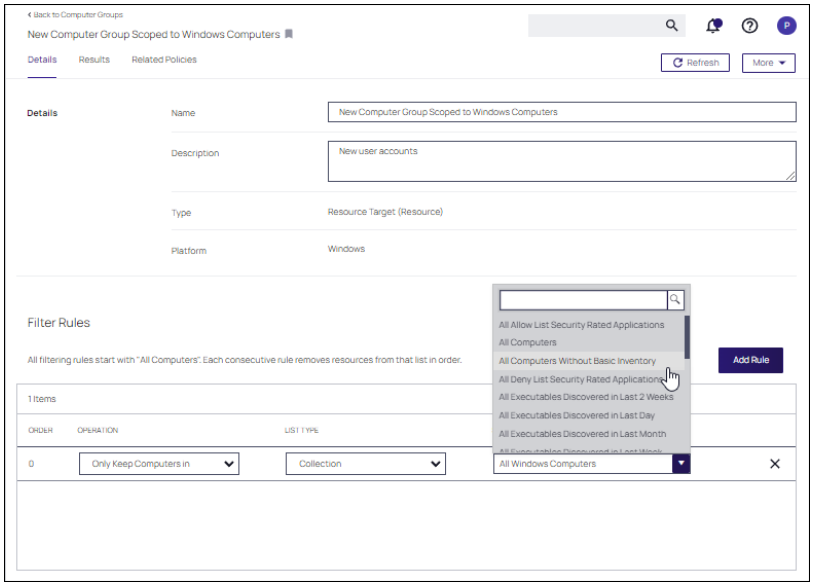
3. From the **Create Computer Group** window, enter a **Name** and **Description** for your new group.



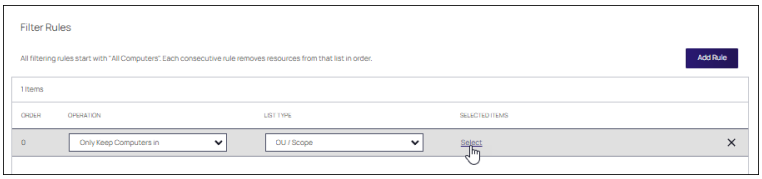
Creating Filter Rules and Collections

To select the machines you want to include within a Computer Group, you must add filter rules that target the appropriate machines on your organization's network. The default filter rule begins with a rule that targets computers within the main OS Computer Group that you selected when you initially created the group. Refer to the Example.

You can add multiple rules per Computer Group. To change existing Computer Groups, you can select **Add Rule** or change the resources already targeted.



1. To narrow your group, click **Add Rule**.
2. Specify the **Operation** behavior, such as:
   - Only Keep Computers in (default)
   - Include Computers in
   - Remove Computers in
3. In the **List Type** column, select from the following options:
   - **Computer List**: Under **Selected Items**, if the label, **Nothing selected** appears, click **Add**. Search for and select computers from the list of registered machines.
   - **Collection**: Under **Selected Items**, click the drop-down list box and choose a collection name such as, All Windows Desktops or All Windows Servers.
   - **OU/Scope**: Under **Selected Items**, click **Select** and choose from the options that appear.



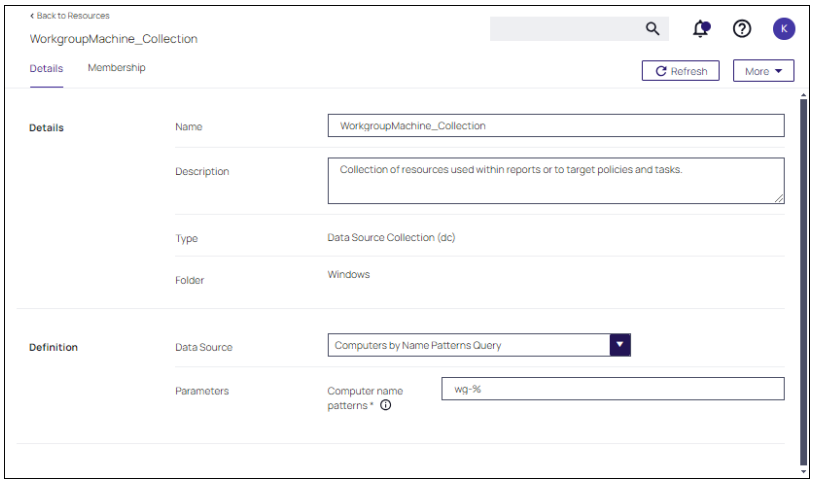
- **Security Group**: Under **Selected Items**, search for and select a security group filter.

4. Click **Save Changes**. Return to the Computer Groups page. The new computer group appears in the table.

Example

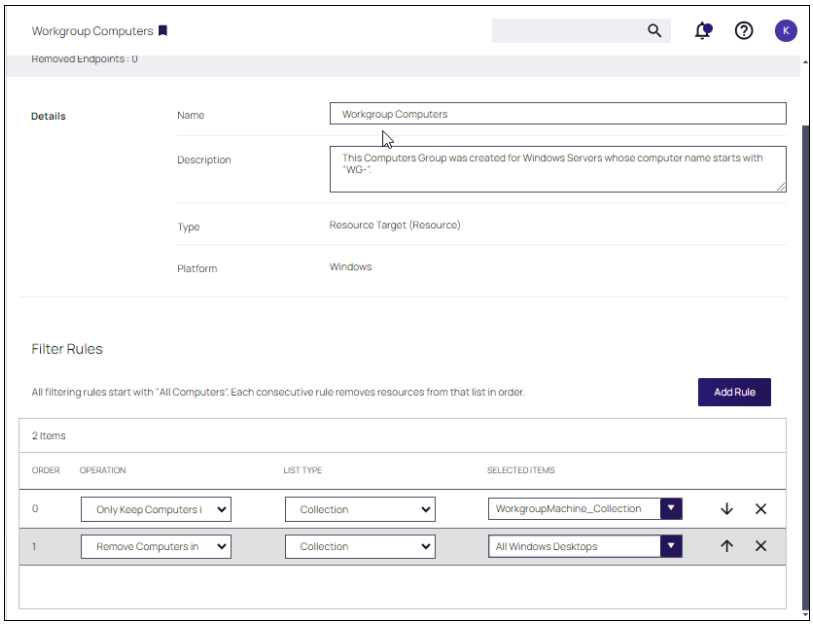
When defining a Collection, you can use the ready-made Items in the Computers Group you have created. (Windows Servers, Windows Desktops, etc.). Or, you can create a custom resources group Different options can be used.

To create a custom resource group, navigate to **Admin** | **Resources**. Select the **Resource Filters** tab and click **Create**. In this example, a Custom group for machines whose machine name starts with "wg-" is created.

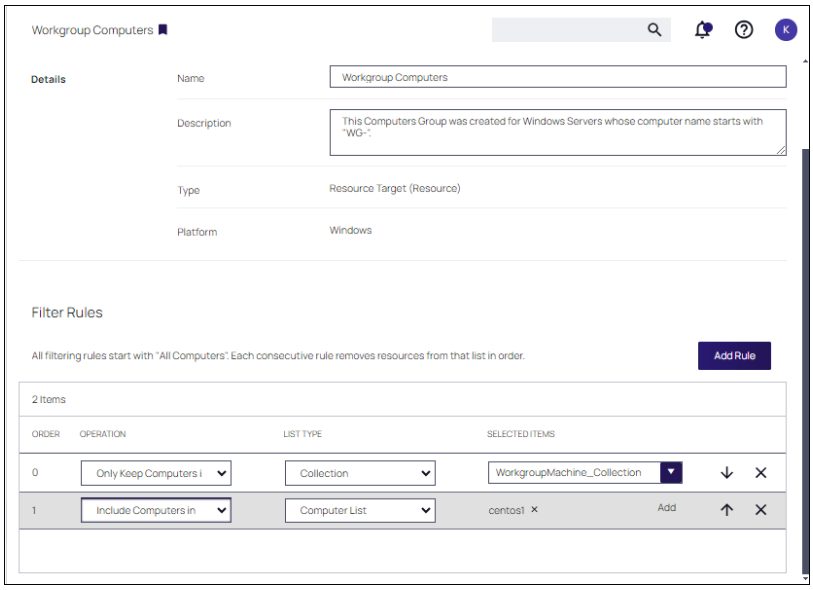


Then, this group is added to the Computers Group.

Important: The first rule must start with **Only Keep Computers**. Then, **Include Computers In** or **Exclude Computers In** rules can be used. For example, you can add computers whose machine name starts with **WG-** and are not Windows Desktops.



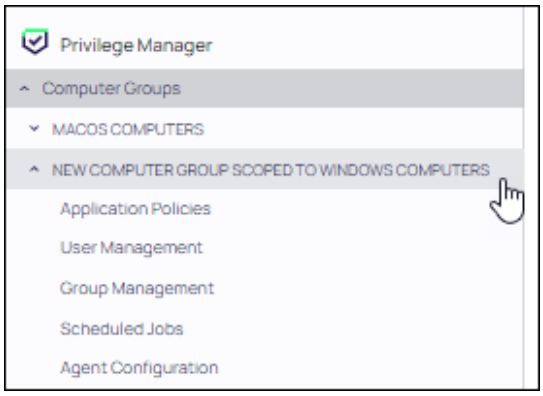
As an alternative to using Collections, you can also use **OU/Scope, Security Group and Computer List** to **Include Computers In**or **Exclude Computers In**. In this example, the collection of computers whose names starts with wg-, and are named centos1 will be members of this group.



Defining Policies, User Management, and Agents

Expand the left navigation tree for the new computer group. Click the available features (**Application Policies**, **User Management**, **Group Management**, **Scheduled Jobs**, and **Agent Configuration**) to further configure the computer group.

For example:



Refer to the following sections:

- Application Policies (Windows, macOS, Unix/Linux)
  - Policies associated with Application Control that you establish using the **Create Wizard** policy.
- User Management (Windows, macOS)
- Group Management (Windows, macOS)
  - Local security control that pertains to specific groups of users.
- Scheduled Jobs (Windows, macOS, Unix/Linux)
  - Client tasks that you designate to run on certain dates and at certain times. Privilege Managersets many scheduled jobs to Active by default.
- Agent Configuration (Windows, macOS, Unix/Linux)
  - Policies that allow global configuration of agent behavior.
    For specific platforms:
    - macOS
    - Unix/Linux
    - Windows

Viewing Computer Groups

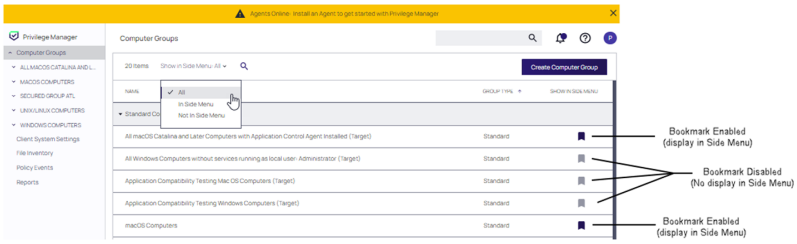
Click **Computer Groups** at the top of the left navigation pane. The Computer Groups table updates to display all currently defined computer groups. Use the **GROUP TYPE** column to change the sort order by group type.

Using Bookmarks

Each computer group has a bookmark setting that can be enabled or disabled. If a bookmark is enabled, it is displayed in the left navigation pane. Disabling a bookmark removes the computer group from the left navigation pane.

The **Show in Side Menu** pull-down controls the display of computer groups in the Computer Groups table with enabled, disabled, or all bookmarks. Selections include **In Side Menu** (i.e., display only bookmarked computer groups in the table), **Not In Side Menu** (i.e, display only computer groups that are not bookmarked in the table), or **All** (display all computer groups in the table).

Note: The setting of **Show in Side Menu** only affects the display of computer groups with specific bookmarks in the Computer Groups table. The bookmark itself determines whether or not it is displayed in the left navigation pane.



Details

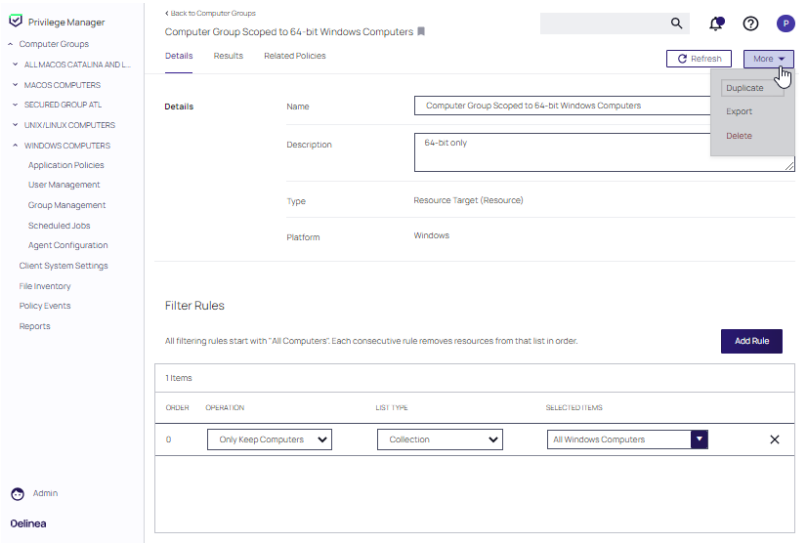
Click any computer group entry in the Computer Groups table. The **Details** page for the selected computer group is displayed. This page includes its name, description, type and platform.

Note: The built-in Computer Groups provided with Privilege Managerare read-only.

Refresh is used to update details after editing. The **More** pull-down provides the ability to duplicate of export a computer group. Exported computer groups are downloaded to the default download directory as a ZIP file.

Filter Rules for the computer group can be defined. All filtering rules start with **All Computers**. Each consecutive rule removes resources from that list, in order.

Refer to Creating Filter Rules.



Results

Click the **Results** tab to view information regarding the resources used with the current rules defined in the Computer Group. Click **Update Results** to update the page if rules are changed.

Note: If a computer is not appearing initiate a Run Policy Targeting Update task. This task runs periodically, but can be triggered immediately.

Related Policies

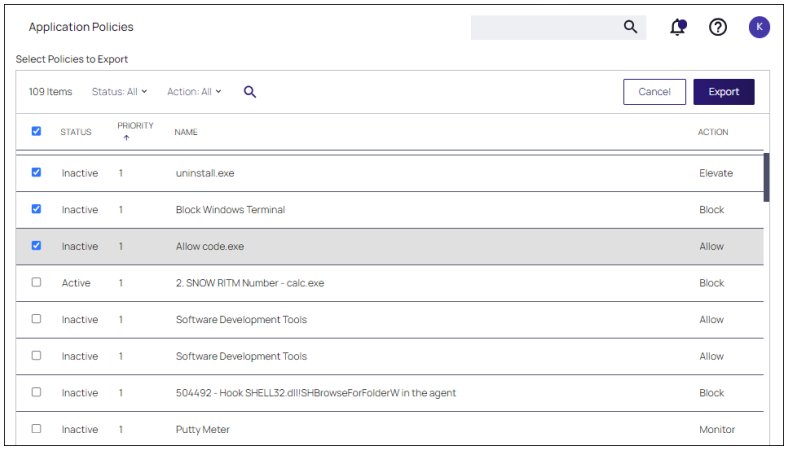
Click the **Related Policies** tab to view the policies currently defined for the Computer Group.

Exporting Policies

Application policies can be exported from the Application Policies page. Prior to exporting a policy, consider:

- If you are exporting policies associated with a custom Computer Group that have been moved to another Privilege Manager instance, you first need to import the Computer Group to allow you to then import the associated policies.
- If you are exporting policies associated with a custom made Secured Group that have been moved to another Privilege Manager instance, you first need to import the Secured Group, its Security Descriptor and Resource Target to allow you to then import the associated policies.

1. Navigate the Applications Policies page in your Computer Group and select **Export**.
2. Enable the check boxes next to each policy to be exported. A select all check box is also available.
3. Click Export.

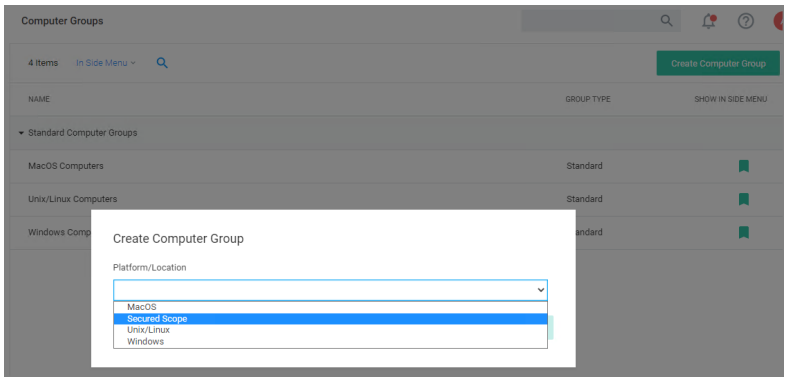


Secured Computer Groups

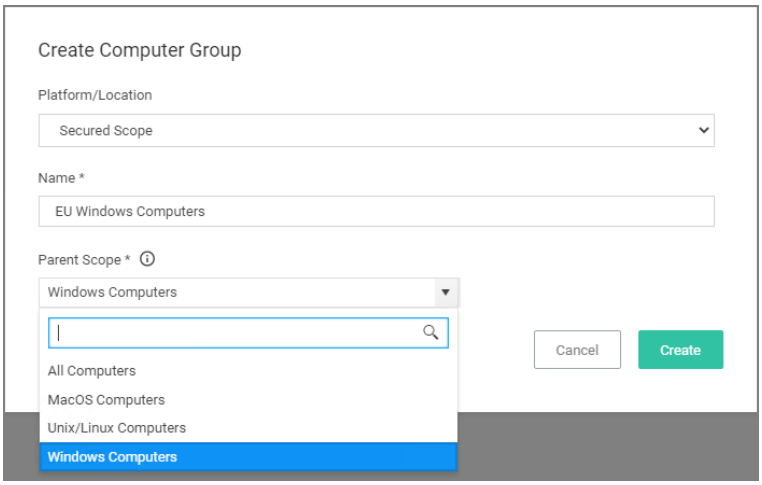
Secured Computer Groups allows Privilege Manager Administrators to create subgroups within the macOS, Linux/Unix, and Windows OS based scopes. These subgroups can target specific geo locations, like all systems based on a specific OS in Asia or Europe.

Creating a Secured Computer Group

1. In your Privilege Manager console in the left navigation menu, click **Computer Groups**.
2. Click **Create Computer Group**.

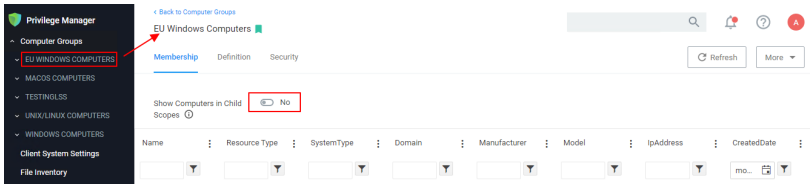


   a. From the **Platform/Location** drop-down, select **Secured Scope.**
   b. In the **Name** field, enter a meaningful name for your use case of this group.
   c. From the **Parent Scope** drop-down, select the parent association based on OS Computer Group. Do not select **All Computers**. The Secured Computer Group is a subset of the parent and has to be scoped to either macOS, Unix/Linux, or Windows Computers.



Once created, the Computer Group page is displayed. By default, the group is added to the left navigation menu of the Privilege Manager console.

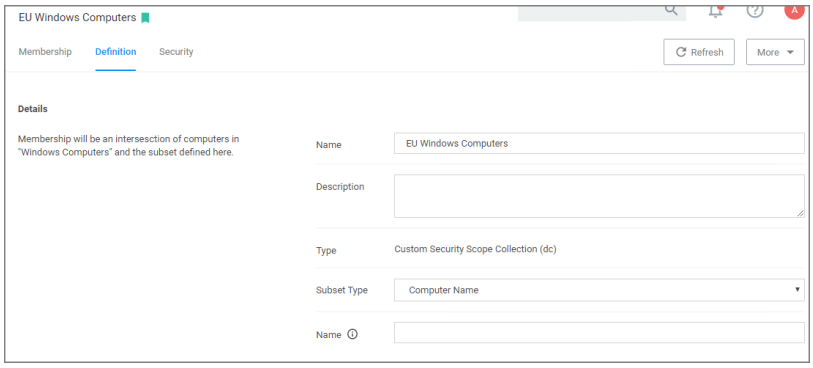
Membership Tab



The **Membership** information will show only the direct members of the group, unless you set the **Show Computers in Child Scopes** switch to **Yes**.

Definition Tab

On the **Definition** tab, you can further define the subset of the group.



Under **Details**, the **Name** and **Description** are reflected as specified when the Computer Group was created.

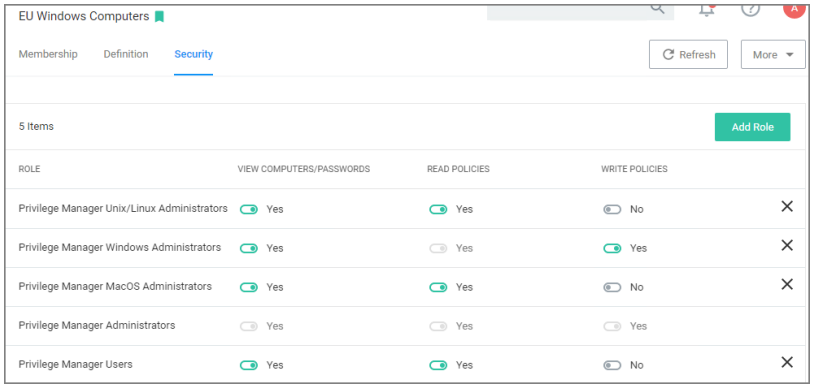
The **Type** is Custom Security Scope Collection (dc).

The **Subset Type** can be changed via drop-down, it defaults to Computer Group, but for definition purposes a Privilege Manager Admin can choose from the options listed in the table below. Based on **Subset Type** selection the last definition field changes:

Subset Type	Specification
Computer List	**Computers** - Click **Add** to select computers to be added from a picker. The picker will show all computers in the environment, only those that are members of the parent collection can be members of this set.
Computer Name	**Name** - Enter the names for the computer to be added. You can type in the exact name of a computer or append/prepend a '%' as a wildcard.
Scope	An **AD domain** to be selected from the list of known AD domains.
Security Group	A **Group** to be selected from a list of resources based on a search by Name option.

Security Tab

On the **Security** tab, roles can be turned on and off for various CRUD operations.



Note: In order for the **View Computers/Passwords** options to be enforced correctly and to use what is defined in the scopes, navigate to **Admin | Security** and open the **Configuration** tab to set the **Resource Security** to **Secured Computer Groups**. Refer to Security Configuration Tab on the **Security** topics page under the Admin Menu section.

Note: If you are using Secret Server as the vault, roles and permissions as defined in Secret Server control who can see which secrets. The Secured Computer Group Security settings only apply to data within Privilege Manager.

Priority Considerations

When setting up Secured Computer groups and policies, the priority settings of those policies needs to be well considered between the parent and child computer groups.

An example of conflicting policies is where a Windows Computer Group may have a policy to block notepad.exe and its child Windows Computer Group has a policy that requires an approval for notepad.exe. In order to make this work, the child Windows Computer Group policy needs to have a higher priority than the parent Windows Computer Group policy. This ensures that the computers in the child group request approval when Notepad is selected and the computer in the parent group blocks Notepad when it is selected.

Scheduled Jobs

Any task targeted to run on endpoints can be run/scheduled from Computer Groups. Open the Computer Group where the job will be scheduled and select **Scheduled Jobs**.

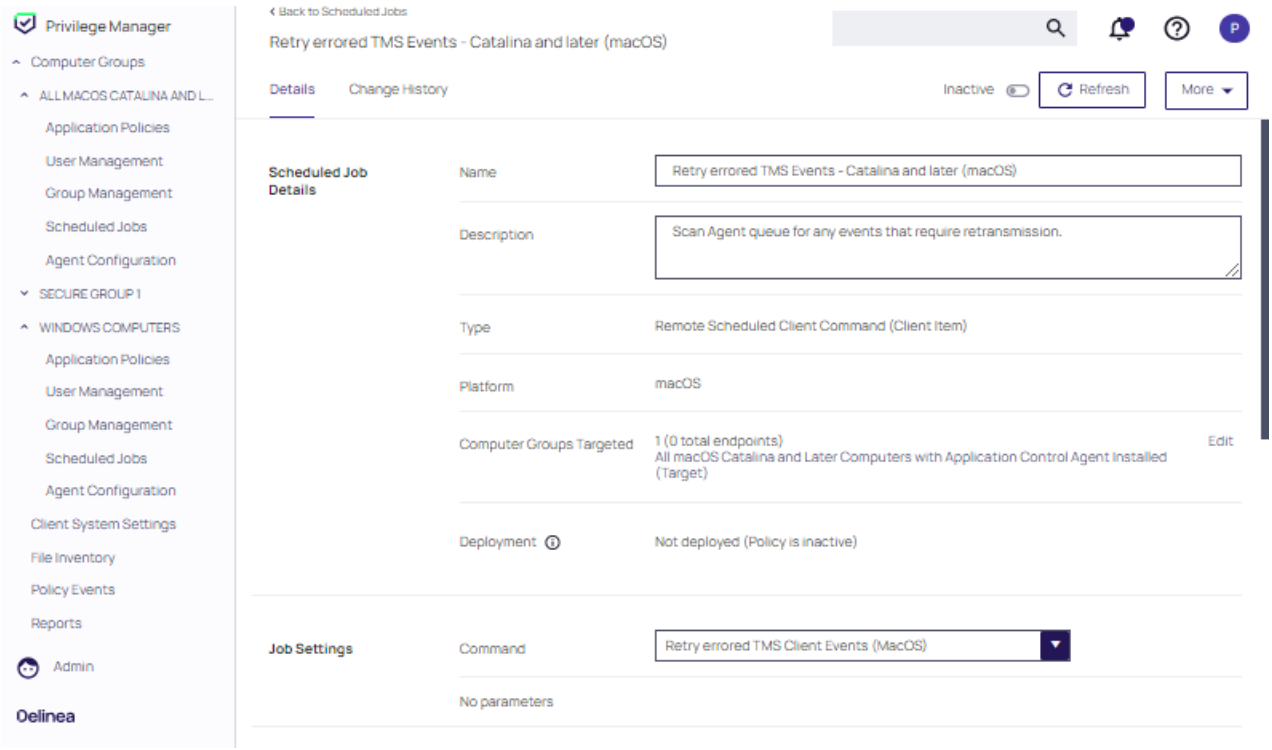
Click any currently configured job. The **Details** tab presents the parameters defined by the job. The **Change History** tab lists the time, date, and description of any update to the job.

The items available at the **More** pull-down allows the job to be deleted or duplicated.

The details of a scheduled job include:

- **Scheduled Job Details** - job descriptors, including deployment status
- **Job Settings** - commands and parameters defined

- **Job Schedule** - time or events that trigger the job
- **Job Conditions** - conditions that affect the triggering of the job



Editing a Scheduled Job

An active or inactive job can be edited on the Details page. Not all fields are editable. Non-editable fields are grayed out.

Click the **Active/Inactive** toggle to change the status of the job. Click **Edit** next to the **Computer Groups Targeted** field to add or remove computer groups to the job.

Use the **If the task is already running, then the following rule applies** pull down at the bottom of the page to affect the rule that triggers the job.

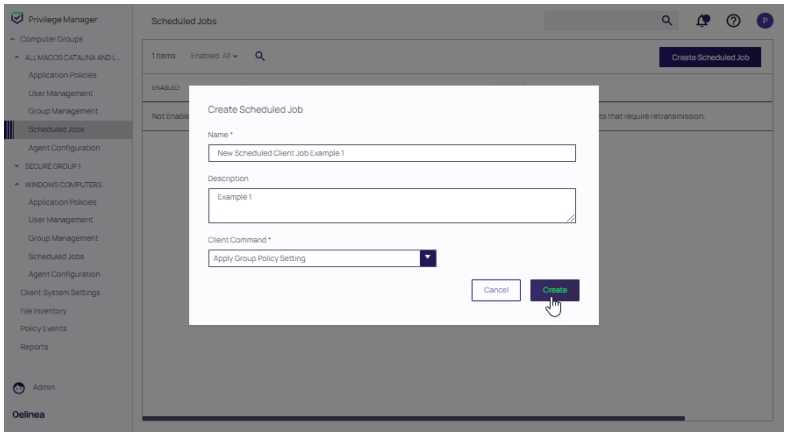
Click **Refresh** at the top of the page to update the job after making changes.

Creating a Scheduled Job

Perform the following steps to create a new job.

1. Select **Create Scheduled Job** at the Scheduled Jobs page.
2. At the **Create Scheculed Job** form, supply a name and description for the job, and select the task that will be run in the job.

3. Click **Create**.



User and Group Management

Each computer group contains all local groups and local users on endpoints with a local security agent installed. When the agent registers, Local Security automatically discovers the local groups that exist on each machine.

Refer to User Management to configure Local users. Refer to Group Management to configure local groups.

Delete Local Users or Groups

Note: This feature is available for Windows computers only.

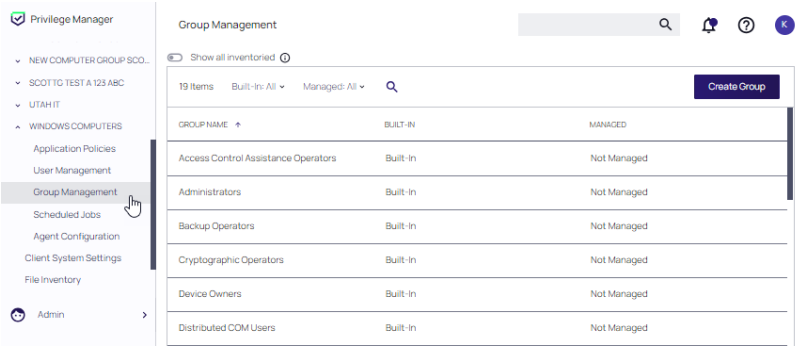
Privilege Manager's Local Security features include provisioning and managing local users and/or groups. The **Local Security Delete Command**, available as a scheduled job, can be used to delete local users and/or groups.

Note: We strongly recommend running this job against one test machine before deploying it to an entire environment.

1. In the computer group with the local users or groups to be deleted, select **Scheduled Jobs**.
2. Click **Create Scheduled Job** in the top right and name the policy.
3. Make the following updates to the job:
   a. In the **Job Settings** section of the form, specify **Local Security Delete Command** in the **Command** field.
   b. In the **User Names** and **Group Names** fields, customize the Local Users and Groups to delete.
   c. At the bottom of the task item, there is a switch to also delete the user's folders from the machine(s). There are also schedules or triggers which can be added to run this task.
   This item will create a Scheduled Task on the endpoint(s) which will run on the Job Schedules assigned in Privilege Manager. This task will find the local user(s) by name, determine if they have an active session, log out the user if there is an active session, delete the user account, and delete the user's User folders, if that additional step is enabled on the Policy. The task will also find the local group(s) by name and delete use local groups.
4. Click **Create**.

Group Management

Every Computer Group is divided into Groups and Users. Both **Groups** and **Users** in this context refer to local accounts and any Azure AD synchronized resources as part of a particular Computer Group.



The Computer Group page lists all local groups on this set of computers, and provides a high-level overview of the selected computer group based on Local Users, Local Groups, and the number of computers in the group.

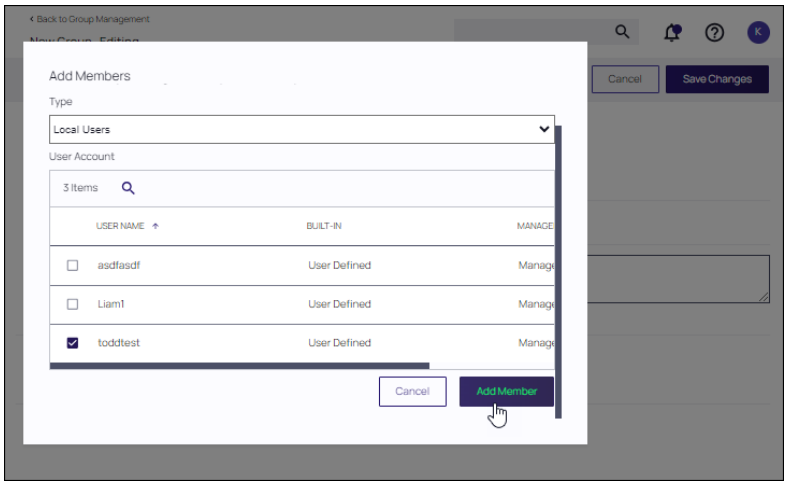
> **Tip:** When an agent registers, Local Security will automatically discover the local groups that exist on each machine.

The Group Management and User Management pages have been configured to load faster by showing the list of managed and built-in users and groups only. Inventoried users and groups will no longer appear by default unless there are less than 200 workstations in that computer group. You can still manage any group or user on those workstations by clicking **Create User** or **Create Group** available in the top right of their respective tables.

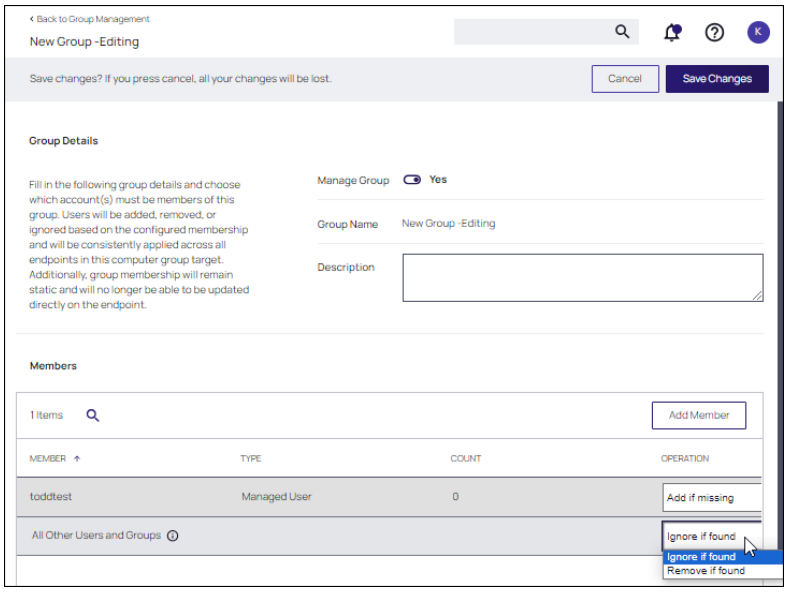
Create New Local Group

To create a new Group,

1. Under your Computer Group, select **Group Management**.
2. Click **Create Group**.
3. Enter a name for your new group.
4. Click **Create**. The Group Details page is displayed. The **Manage Group** switch is by default set to **Yes**.
5. Click **Add Member**.

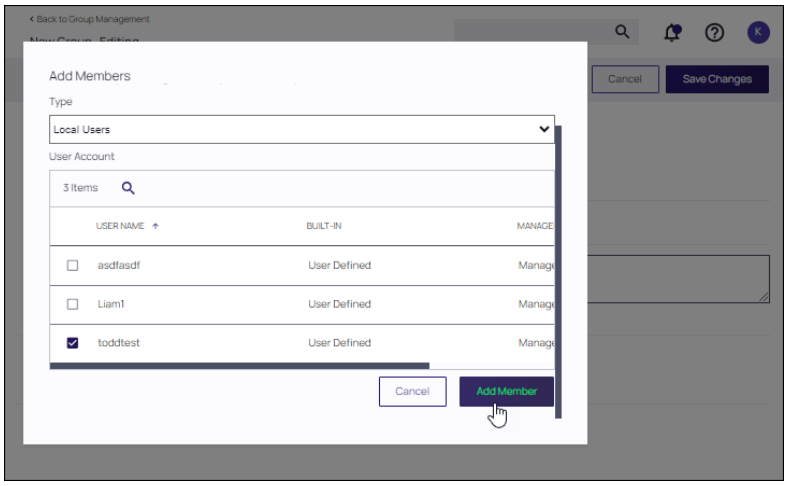


6. From the **Type** drop-down, select either
   - Domain User
   - Domain Group
   - Local Users
   - Local Users (Manual Entry)
   - Local Users (Regex)



7. On the **Add Member** dialog, select from the available resource items.
   for **Domain User** or **Domain Group**. For **Local Users**, select the user from the list as shown in the example image below. **Local Users (Manual Entry)** allows you to enter specific local user names.
   Local Users (Regex) allows you to enter specific local user names with Regex expressions.

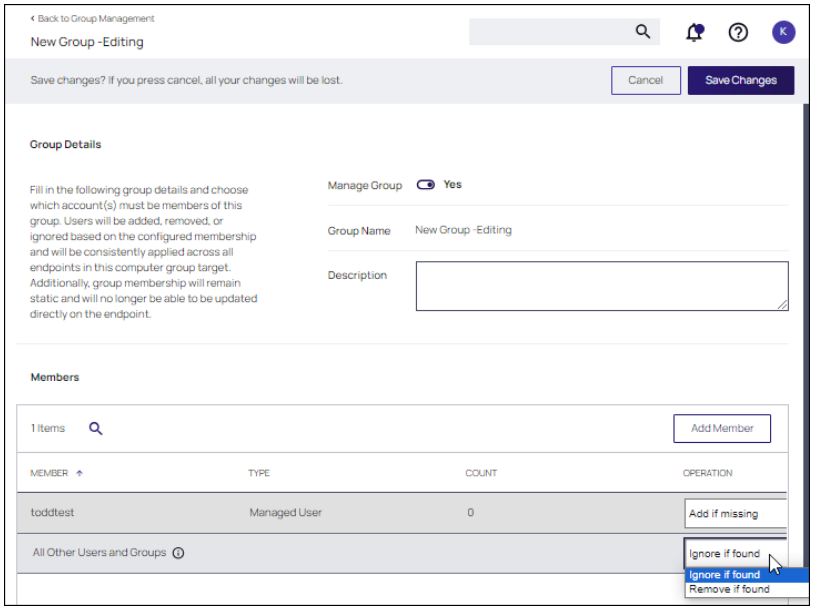
> ⚠ You must use specific and restrictive regex. We cannot guarantee that your expression will never include an unintended user. Please validate the expression yourself with one of the many online regex testers, and check group members regularly.



8. Click **Add Member**.
9. The User Group Details page is displayed. Review all settings prior to clicking **Save Changes**. Refer to Manage Local Groups.

Manage Local Groups

Managing a local group means that you determine which user accounts are in the group. In other words, if a group is being managed, the group membership will remain static and will no longer be able to be updated directly on the endpoint. Before adding users to any group, make sure you really want all those users in that particular group. Any exact group membership setting is rolled out to ALL endpoints in that computer group.



Details tab

If a local group is not managed, the **Manage Group** is set to **No**. To manage the group, set **Manage Group** to **Yes** and click **Save Changes**, then **Yes** to confirm. Changes to these settings may take up to 15 minutes to update on your endpoints.

When managing a group, existing members and any that have been added to the policy will appear in the Members table. Users will be added, removed, or ignored based on the configured membership and will be consistently applied across all endpoints in this computer group target. From the drop-down, choose which operation to perform if an account (user) is found on the endpoint. The following options can be selected:

- Ignore if found
- Add if missing
- Remove if found

Using **Remove if found** for **All Other Users and Groups** instates exact group membership and **Ignore if found** cannot be used on individual accounts that are part of that group. Note that, if **exact group membership** is used, an account that is initially listed as **Ignore if found** switches to **Remove if found** as part of the group membership. Individually specified accounts can be set to **Add if missing** in those groups. Also refer to Non-Managed Local Users in Group Management for details about non-managed users in managed groups.

Note: Once saved, group membership is permanently defined. Updates made directly on the endpoint that break this policy will be immediately reverted.

The last row defines what action to take **on all other users and groups**. This ensures exact membership can be defined and any other users or groups can be automatically removed.

Statistics tab

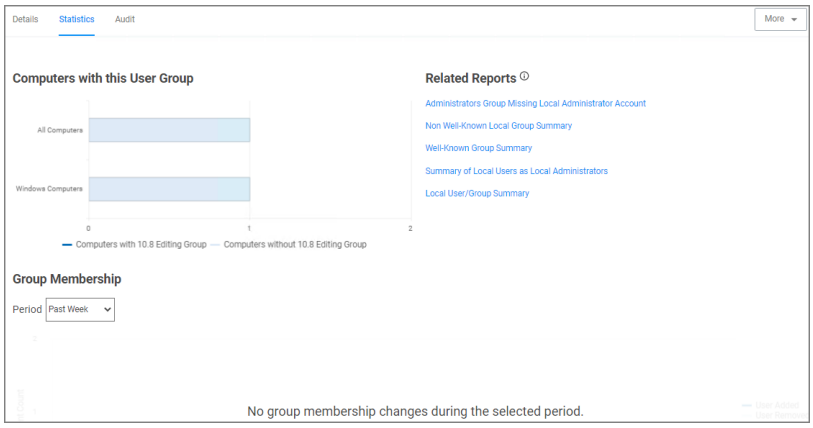
The **Statistics tab** for a local group highlights some quick visual statistics and links you to relevant reports based on key factors like how many computers from your network are included in this group and whether there have been changes made to the group's membership within the specified period. Click on these graphs to drill down into more details.

Note: The reports in the “Related Reports” sections are scoped to only include endpoints in the current computer group. To view reports across all computers, go to the Reports section of the product.

Audit tab

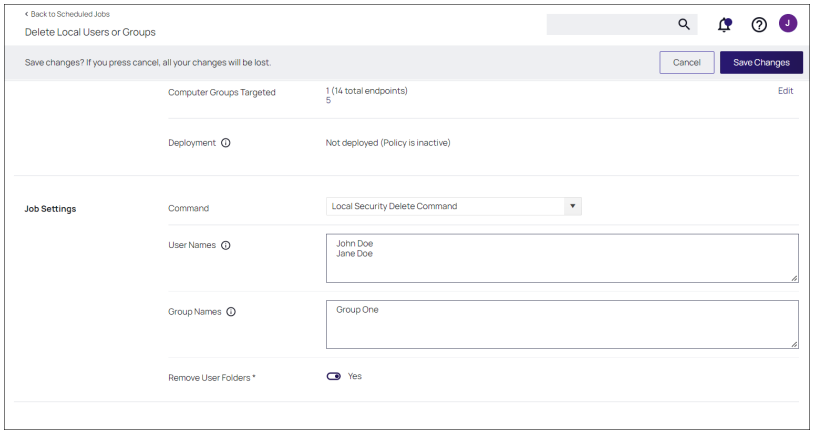
The **Audit tab** is where you will find an audit record of all membership additions and deletions that have been made to your local groups.

When the agent makes a change to the group based on how the user has configured the group in Privilege Manager, that change is recorded in Audit, as a user is **Added** or **Removed**.



Delete Local Users and Groups

Privilege Manager allows you to delete local **User Names** and **Group Names** via the Scheduling function. You can also delete user folders; the **Remove User Folders** switch (set to **Yes** by default) deletes the associated user folders in c:\users.



To delete **User Names** and **Group Names**:

1. From the left navigation pane of the Privilege Manager console, select **Computer Groups**.
2. From a computer group, select **Scheduled Jobs**.
3. Click **Create Scheduled Job**.
4. From the **Create Scheduled Job** window, enter a **Name** and **Description** - ensuring each is meaningful and aligned with the task you are scheduling.
5. From the **Client Command** drop-down list box, select **Local Security Delete Command**.
6. Click **Create**.
7. Scroll to the **Job Settings** section of the page that opens, entering text in the appropriate **User Names** and **Group Names** fields. Enter one name per line, pressing ENTER to add multiple entries in one or both fields.

> **Note:** Neither the **User Names** nor **Group Names** fields are case sensitive; however, you must spell each name correctly. For example, entering *JOHN DOE*, *john doe*, or *John DoE* will delete user: *John Doe*. Entering *John Doee* will not remove the *John Doe* user. Also, you cannot append the computer name_domain name to a user name; *PMQA1Z-1234-1\JohnDoe123* will not remove the *JohnDoe123* user. Similarly, relative to **Group Names**, entering *GROUP ONE*, *group one*, or *Group OnE* will delete: *Group One*. Entering *Group 1* will not remove the *Group One* group name.

8. Accept the default **Yes** position of the **Remove User Folders** switch to delete the associated user folders (c:\users). Slide this switch to the left or **No** position if you do not want to delete these folders.
9. To schedule the job run frequency, click **Add Trigger**. Here, you can establish run dates and times, managing the job schedule using Privilege Manager. Alternatively, you can disregard **Add Trigger**, running scheduled jobs on an ad hoc basis from the agent workstation.
10. To store your updates, click **Save Changes**. The **Inactive** switch appears near the top right of the page. You can slide this switch to the right, activating the scheduled job.

Local Security

Local Security in Privilege Manager allows customers to:

- discover all local accounts and groups that exist on endpoints.
- provide membership control of those accounts on endpoints.
- allows to take complete ownership of the local credentials by enforcing password rotation for all accounts on those endpoints.
- use best practices when it comes to locking down the network from malicious endpoint attacks that exploit unsecured administrative access.

Local Security is made up of

- Computer Grops
- Local Groups
- Local Users

Under **Reports**, various Local Security reports and summaries are available.

Computer Groups

These so called resource targets (as configured in Application Control) are specified sets of computers that meet certain criteria, that are targeted by certain policies and scheduled tasks.

Each computer group contains all local groups and local users on endpoints with a local security agent installed. When the agent registers, Local Security automatically discovers the local groups that exist on each machine.

Local Groups

Groups are created and managed under the Group Management menu node.

Each local group has a list of local users that exist in that specific group. From that list you can see

- how many groups each user account is a member of.
- whether the user account is built-in or user-defined.
- whether or not the account itself is managed.

Local Users

Users are created and managed under the User Management menu node.

Setting up a local user account with password rotation means that the account is a managed account within Privilege Manager.

Local Security Reporting

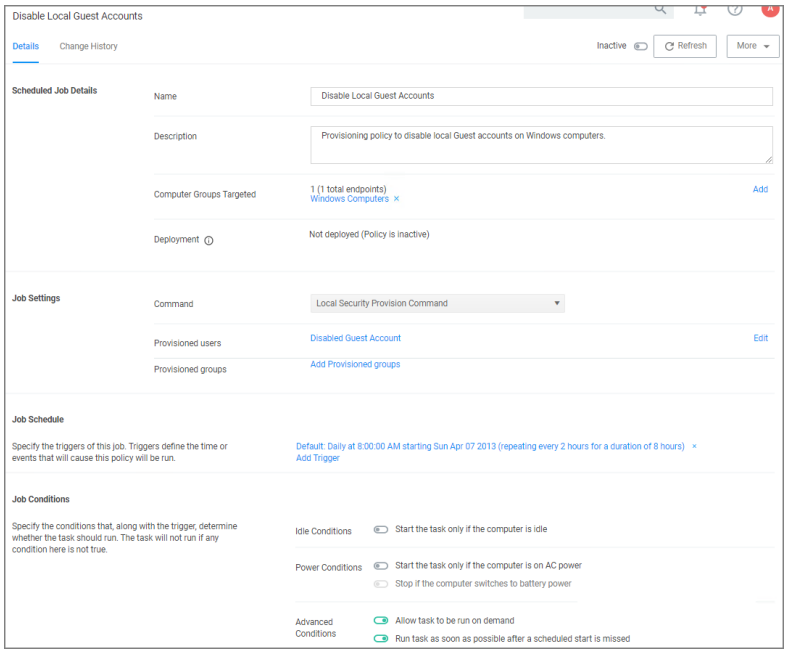
Under Reports various Local Security reports and summaries are available.

Disable Local Guest Accounts

To disable the guest account on computers that have the Local Security Agent installed, enable the **Disable Local Guest Accounts** remote scheduled client command. This is an out-of-the-box policy; you do not need to make any configuration changes to this policy.

To enable the policy:

1. Under your **Computer Group**, navigate to **Scheduled Jobs**.
2. From the Scheduled Jobs list, select **Disable Local Guest Accounts**.

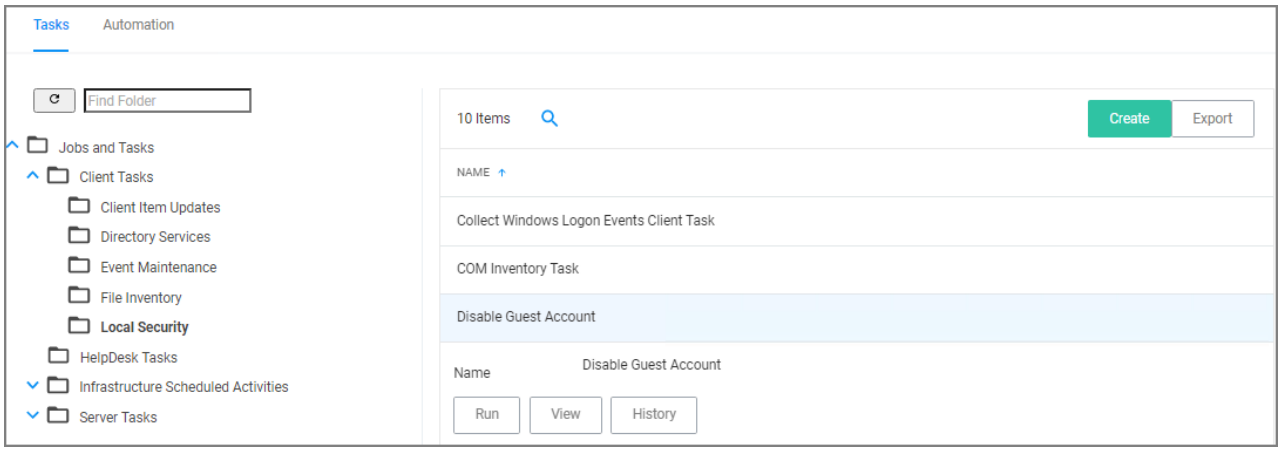


3. Set the **Inactive** switch to **Active**.

If you wish to customize any aspects of the default behavior, create a copy and edit the copied policy.

The Disable Local Guest Accounts policy uses the Local Security task **Disable Guest Accounts**. If you wish to run the task on demand follow these steps:

1. Navigate to **Admin | Tasks**.
2. On the Tasks tab open the folder tree to **Client Tasks | Local Security**.
3. Select the **Disable Guest Account** task.



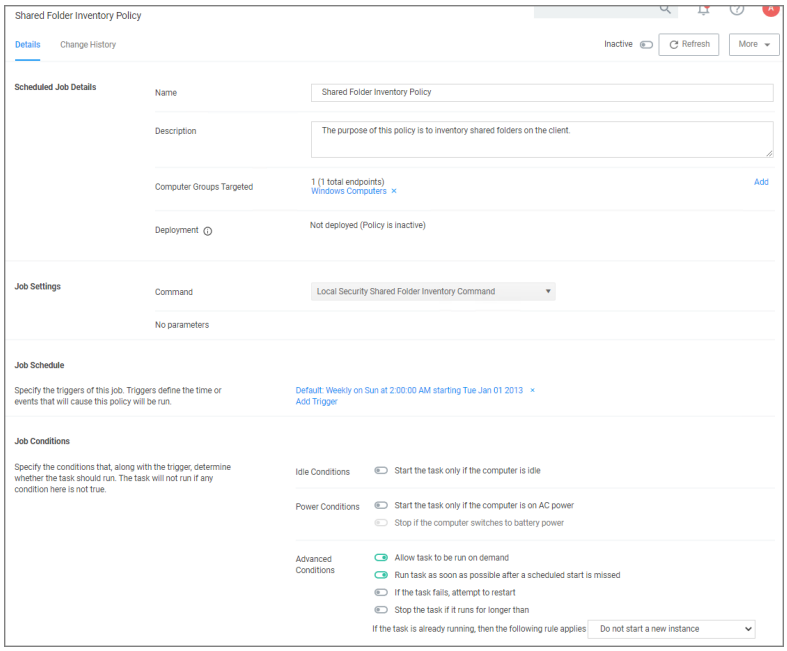
4. Click **Run**.

Shared Folder Inventory

To inventory shared folders on computers that have the local security agent installed, enable the shared folder inventory policy. This is an out-of-the-box policy; you do not need to make any configuration changes to this policy.

Enable the Policy

1. Under your **Computer Group**, navigate to **Scheduled Jobs**.
2. From the Scheduled Jobs list, select **Shared Folder Inventory Policy**.



3. Set the **Inactive** switch to **Active**.

Group Membership

This topic describes types of membership groups and how to establish them.

IT administrators can create user and group accounts. The names of the users associated with specific groups appear in the **Members** table on the primary page for each group, which is accessible via **Group Management** in the Privilege Manager left navigation pane. The **Type** field in the **Members** table displays the *managed user* status. More specifically, the **Type** field can include the following memberships:

- Domain Group
  - Group of users from AD
- Domain User
  - Single users from AD
- Built-in
  - User shipped with the OS
- Managed User
  - User actively managed by Privilege Manager
- Named User
  - User manually added to the group by name and, therefore, not selected from an existing list of users.
- Unmanaged User
  - User that is inventoried or formerly Managed

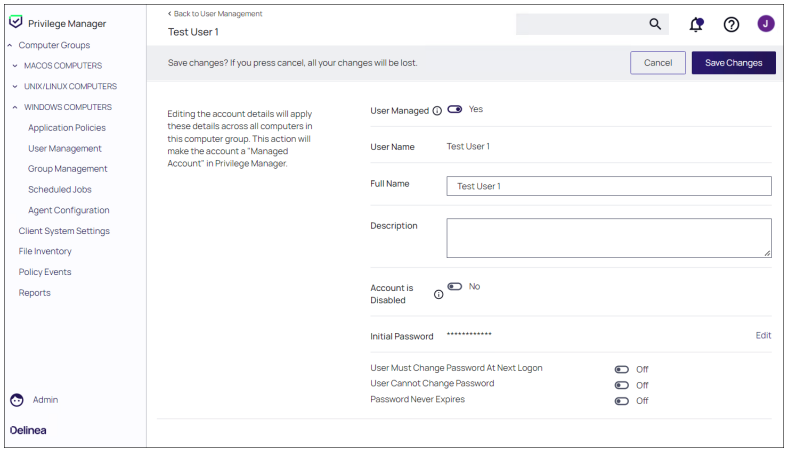
Each membership comprises distinct users, and each membership is significant. The **Domain Group**, **Domain User**, and **Built-in** user memberships populate the **Type** field based on the explanations above.

In the spirit of ensuring a solid understanding, this topic focuses on the **Managed User**, **Named User**, and **Unmanaged User**, which are a subset of the **Local User** category. This topic provides insight and clarity on how each populates the **Type** field.

User Management

To add a user:

1. Navigate to **Windows Computers | User Management**.
2. Click **Create User**.
3. From the **Create Managed User** window, enter a **Username**.
4. Click **Create**. A new page opens, displaying **User Details**.
5. Slide the **User Managed/Not Configured** switch to the right or **Yes** position, thereby applying this account across all endpoints in the computer group. This action also reveals additional fields.
6. Click **Edit** to modify the **Initial Password**.
7. Type a password in the first field and, in the second field, confirm the password by retyping this entry. The password must include an uppercase letter, lowercase letter, number, and symbol.
8. Click **Save Password**.
9. Click **Save Changes**. The **Save Changes** button becomes a **More** drop-down list box. You can click **More** and choose **Delete** to remove this account if needed.

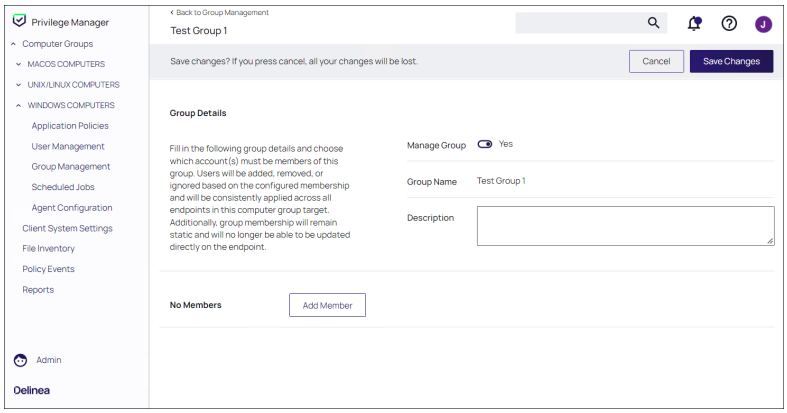


Group Management

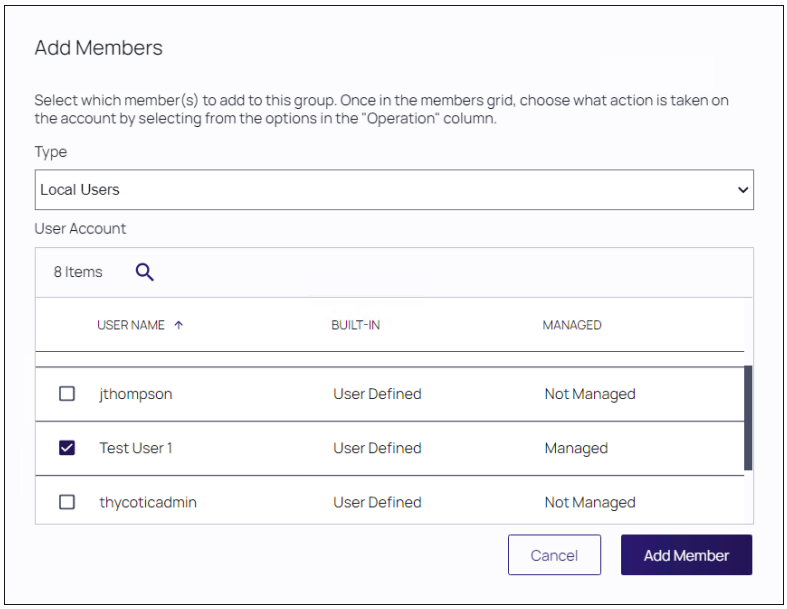
Managed User

To establish and view a Managed User:

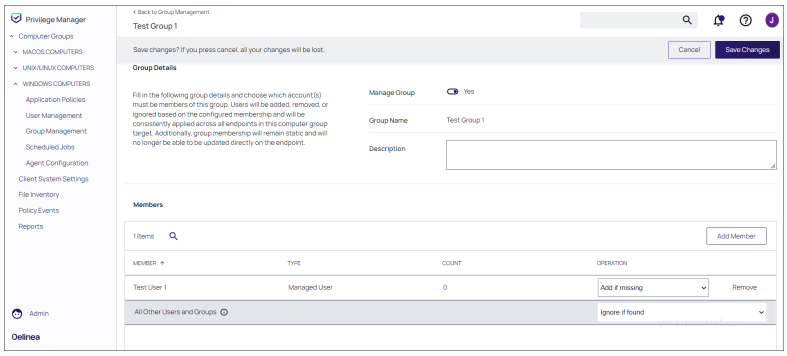
1. Navigate to **Windows Computers | Group Management**.
2. Click **Create Group**.
3. From the **Create Managed Group** window, enter a **Group Name**.
4. Click **Create**. A new page opens, displaying **Group Details**.
5. Click **Add Member**.



6. From the **Type** drop-down list box in the **Add Members** window, select **Local Users**.
7. In the lower section of the window, scroll then find and select the checkbox associated with the user you added.
8. Click **Add Member**.



9. System functionality returns to the previous page. From the **Members** table, you can view the record associated with the user you added. **Managed User** appears in the **Type** field associated with this user.
10. Click **Save Changes**.



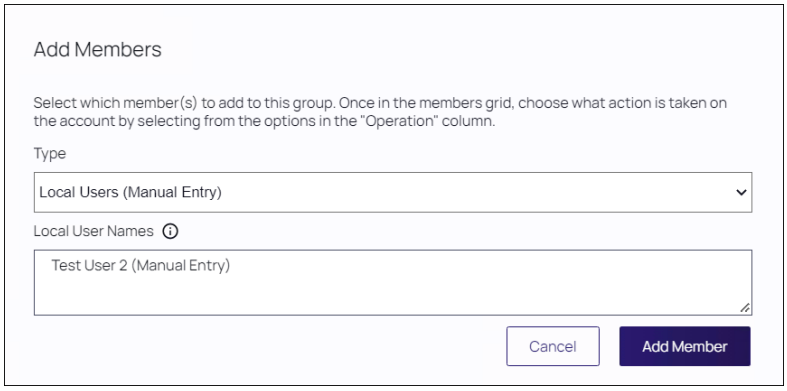
A message appears: **Group membership changes will occur automatically when the endpoint receives the policy or when any membership changes occur directly on the endpoint**.

11. Click **Yes** to proceed.

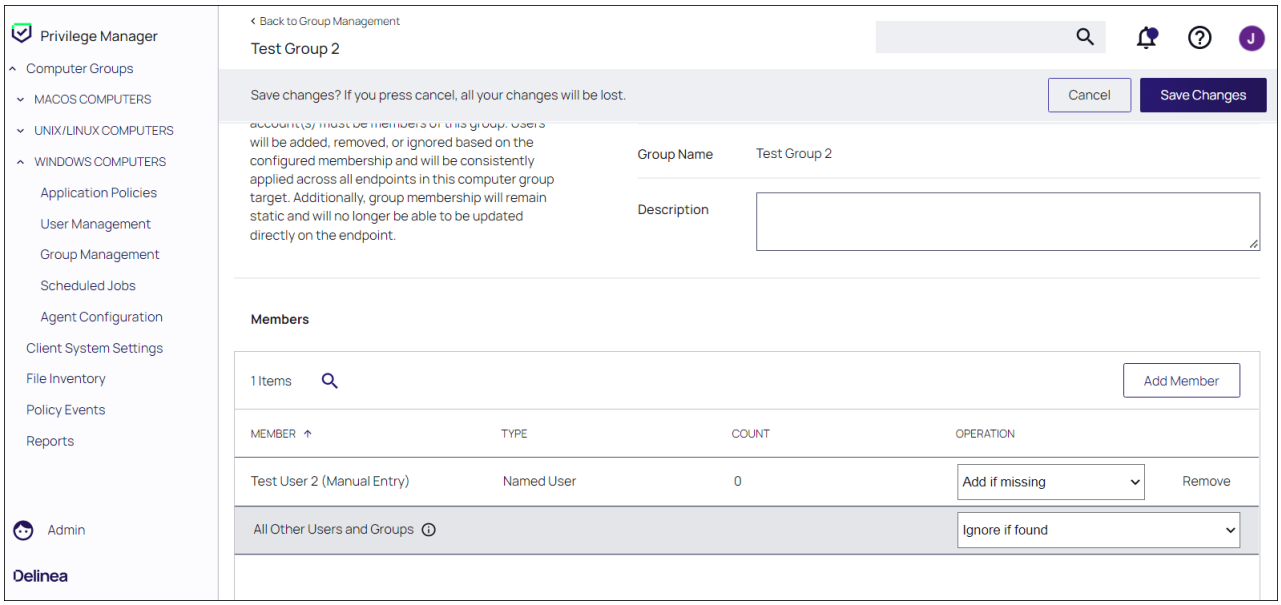
Named User

To establish and view a Named User:

1. Navigate to **Windows Computers | Group Management**.
2. Click **Create Group**.
3. From the **Create Managed Group** window, enter a **Group Name**.
4. Click **Create**. A new page opens, displaying **Group Details**.
5. Click **Add Member**.
6. From the **Add Members** window, click **Local Users (Manual Entry)**.
7. Enter one name per line, if adding multiple users.
8. Click **Add Member**.



9. System functionality returns to the previous page. From the **Members** table, you can view the record associated with the user(s) you added. **Named User** appears in the **Type** field associated with this user.
10. Click **Save Changes**.



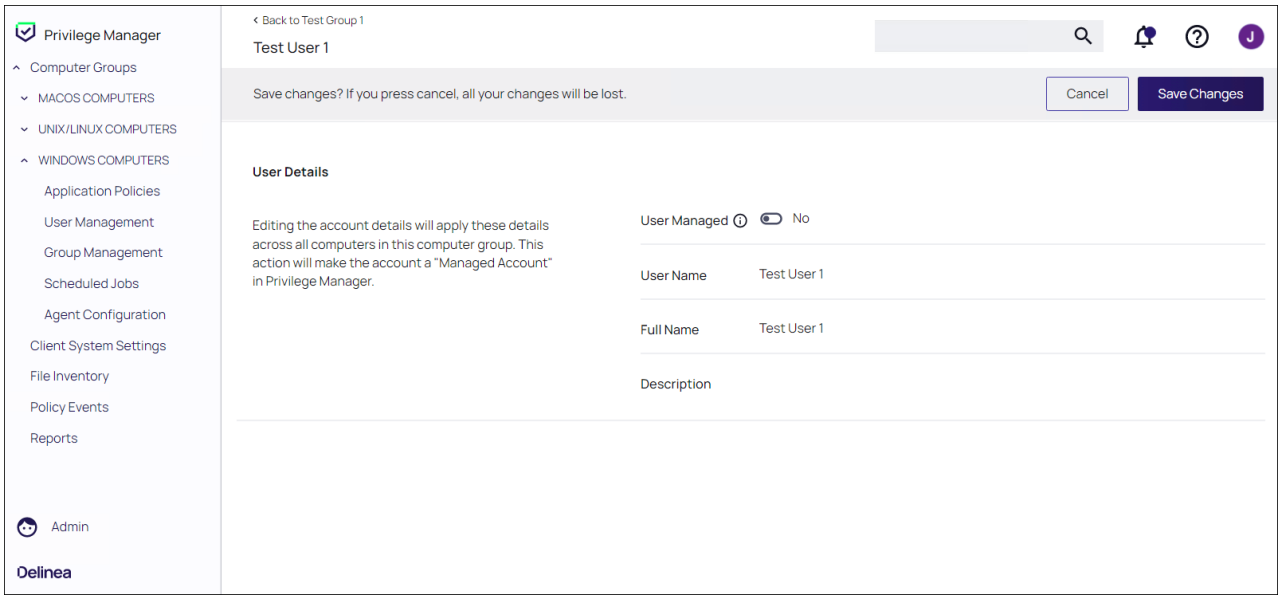
A message appears: **Group membership changes will occur automatically when the endpoint receives the policy or when any membership changes occur directly on the endpoint**.

11. Click **Yes** to proceed.

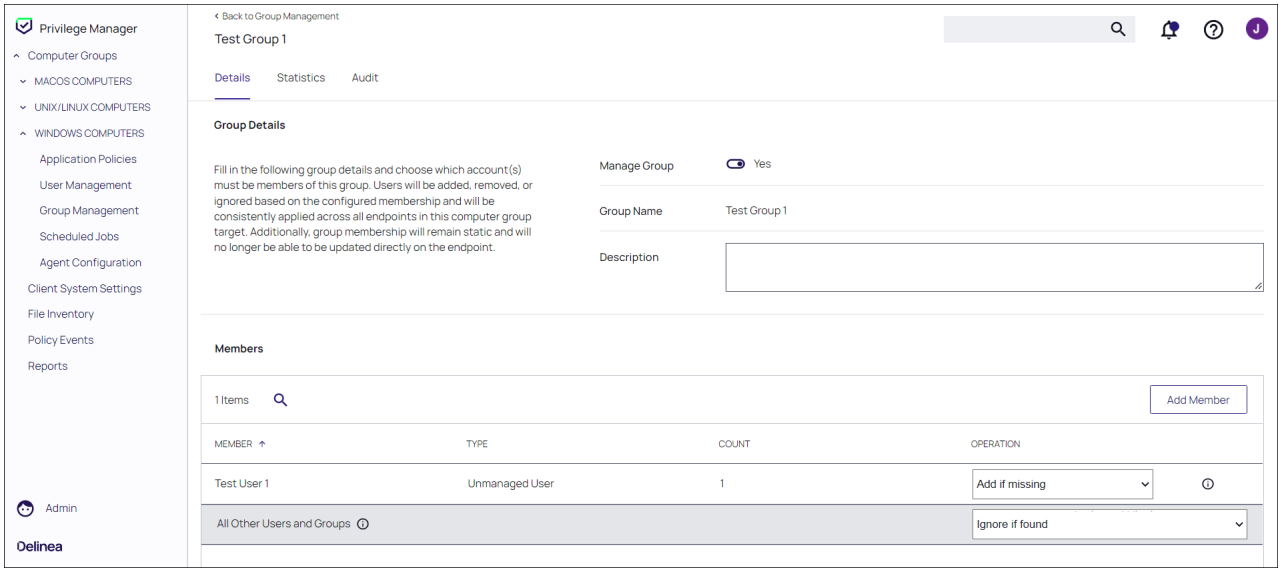
Unmanaged User

To establish and view an Unmanaged User:

1. From the left navigation pane, click **Group Management** then select a group.
2. Access the **Members** table and click the Managed User you created.
3. System functionality launches you to the **User Management** page for this user.
4. Slide the **User Managed** switch to the left or **No** position.
5. Click **Save Changes**.



6. Click the **Back to** breadcrumb link near the top left of the page.
7. The **Type** field now displays **Unmanaged User**.



Migrate Local Security Policies

The migration path to the latest Local Security implementation provides an analysis report of issues like missing account credentials, or accounts that are not unique across targets, which can then be remediated before the migration.

> **Note:** Delinearecommends to use a Professional Services engagement when migrating local security to Privilege Manager 10.7 or newer.

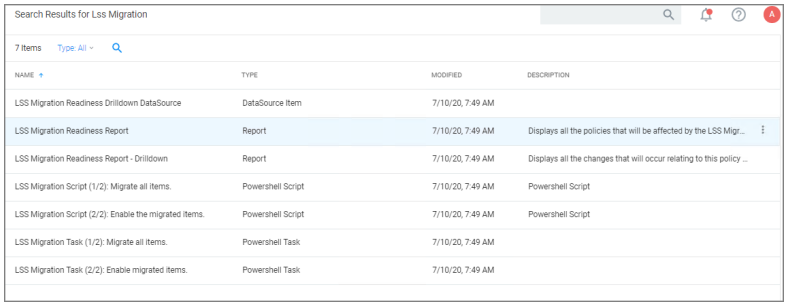
Before any migration is performed, make sure to backup your Privilege Manager database.

Migration Steps

Starting with Privilege Manager v10.7 the LLS Migration Readiness Report is available. The report is generated after an upgrade to v10.7 or higher from any previous Privilege Manager version.

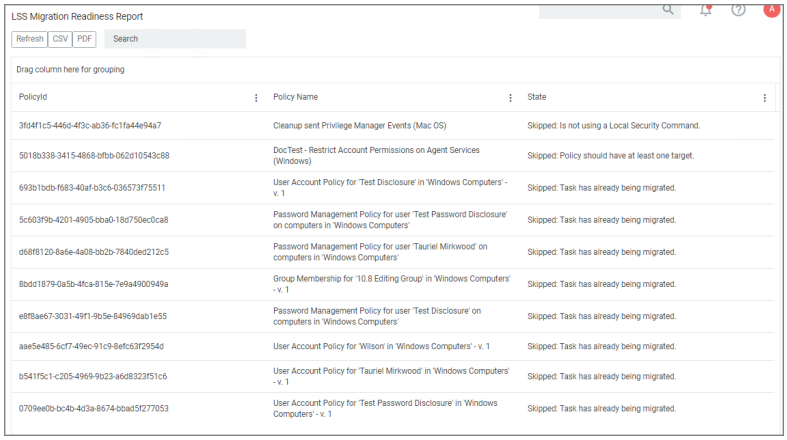
To access the LSS Migration Readiness Report, follow these steps.

1. From anywhere in the Privilege Manager console search for LSS Migration.



   The search does show all LSS Migration labeled results found in Privilege Manager. As the image shows, there are two related reports and tasks.

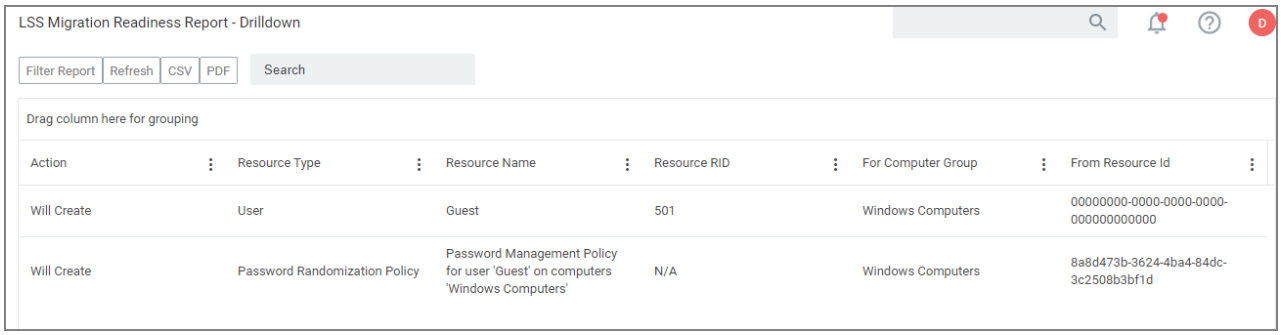
2. Select **LSS Migration Readiness Report**.
3. The report shows a table containing Policy IDs, their Name, and the current migration status.



   The migration state can be:

   - Ready for migration.
   - Skipped: Is not using a Local Security Command.
   - Skipped: Task has already been migrated.

4. To learn more about items that are listed as *Ready for migration* click on the item in the table. This opens up the **LSS Migration Readiness Report - Drilldown** report.



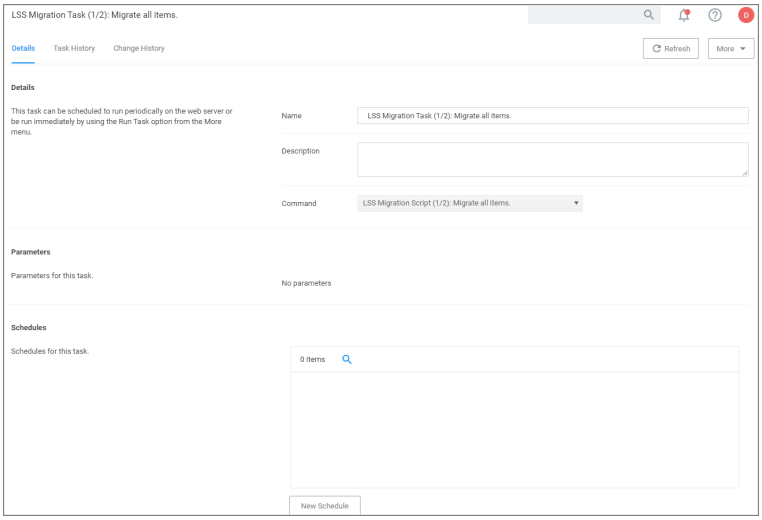
The drilldown report shows the Action to be performed for that particular item during the migration.

For example: The data shown in the image above indicates that two items will be created in Privilege Manager's Local Security. One item is a *User* the other a *Password Randomization* entry. For the user the item is created with **Resource Name** of *Administrator* and the **Resource RID** will be *500*. It further shows that the action will be done **For Computer Group** and **From ResourceID** as indicated.

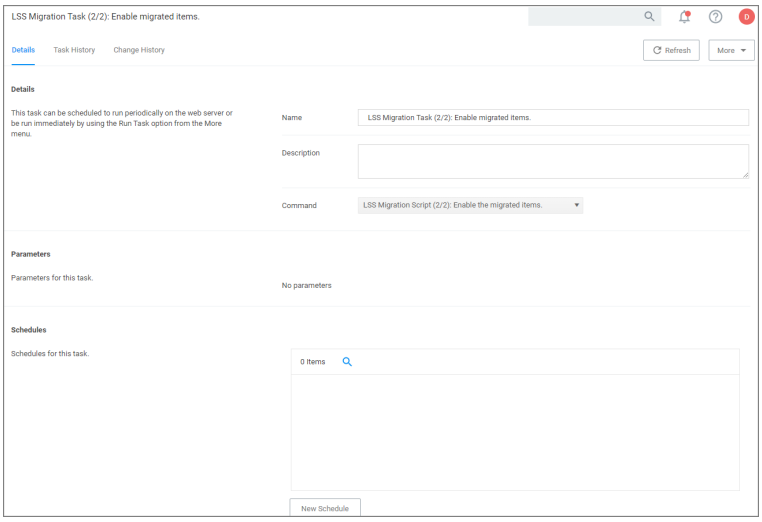
During the report creating, Privilege Manager will find and resolve conflicts that might be caused by many policies targeting the same computer group with the same user/group, or multiple password rotation policies for the same user. The LSS migration script resolves these conflicts in a way that respects the logic of the initial policy set-up, and comply with the new model for the data.

5. If there aren't any conflicts and all items found can be migrated, use the LSS Migration tasks to migrate and then enable to items pertaining to Local Security. This is a two step process, first migrate then enable.

   a. Search for LSS Migration Task (1/2): Migrate all items.



b. After all items are migrated, run the LSS Migration Task (2/2): Enable migrated items.

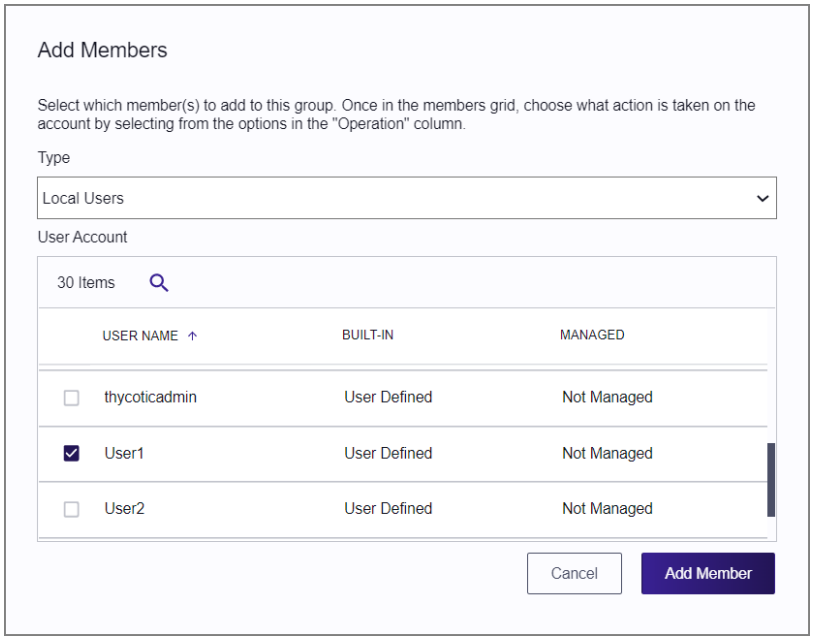


Either of these tasks can be edited, to have parameters or schedules defined.

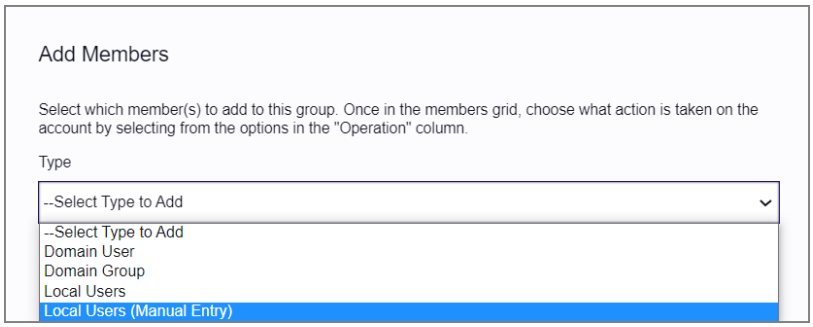
Non-Managed Local Users in Group Management

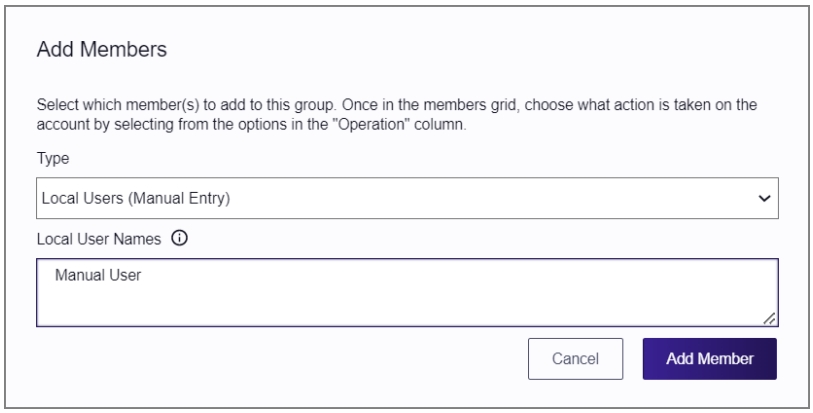
This feature allows for group management of local users that are not managed by Privilege Manager.

When users are added to a group, the modal indicates if their status is managed or not managed:

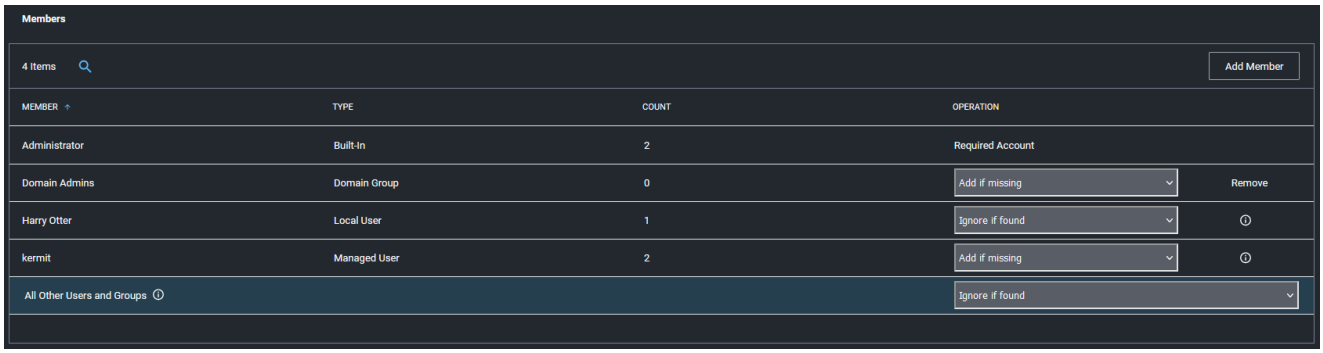


To create an un-inventoried local user to add to a group, select **Local User (Manual Entry)**.





The new view of a Group Management Policy is below.



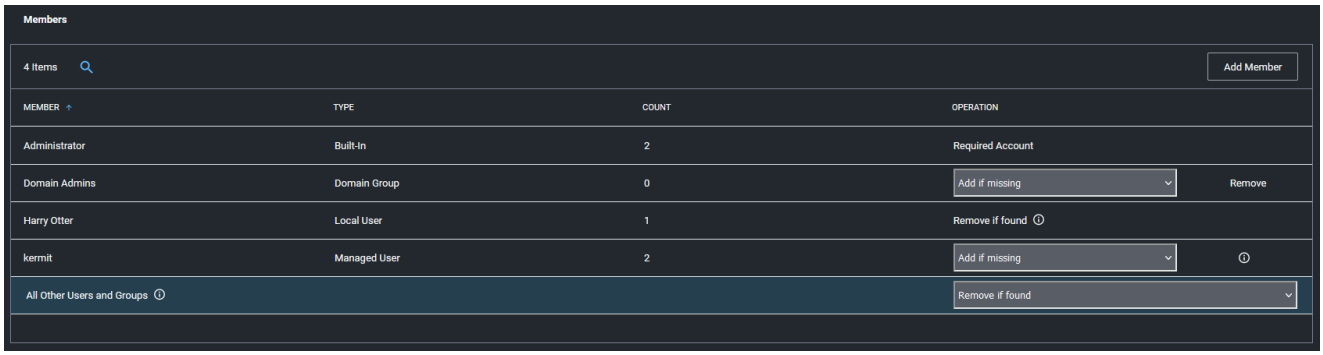
Notice that both Harry Otter and kermit are local users on machines in this Computer Group. However, the kermit account is managed by Privilege Manager and Harry Otter is not.

Even though the Harry Otter account is not managed by Privilege Manager, the group membership definitions can still be defined to **Ignore if found** or **Add if missing**. This allows Privilege Manager administrators to be able to manage the account in a Group Management Policy without having to manage (or provision) that local user on all machines in the Computer Group. If the unmanaged local user is set to **Add if missing**, the user will only be added to the local group on the machines where this local user already exists. This allows Privilege Manager administrators to manage local users without having to provision those users on all machines in the Computer Group.

This functionality is only available when the **All Other Users and Groups** are set to **Ignore if found**.

When **All Other Users and Groups** are set to **Remove if found**, the Group Management requires exact membership - the membership definitions will be the same for all machines in this Computer Group. When this is set, each individual user's membership must be specifically defined. In this mode, the group management of unmanaged local user accounts is not allowed. When **All Other Users and Groups** are set to **Remove if found**, local users must be managed by Privilege Manager (which provisions the account on all machines in the Computer Group) to have their local group membership defined.

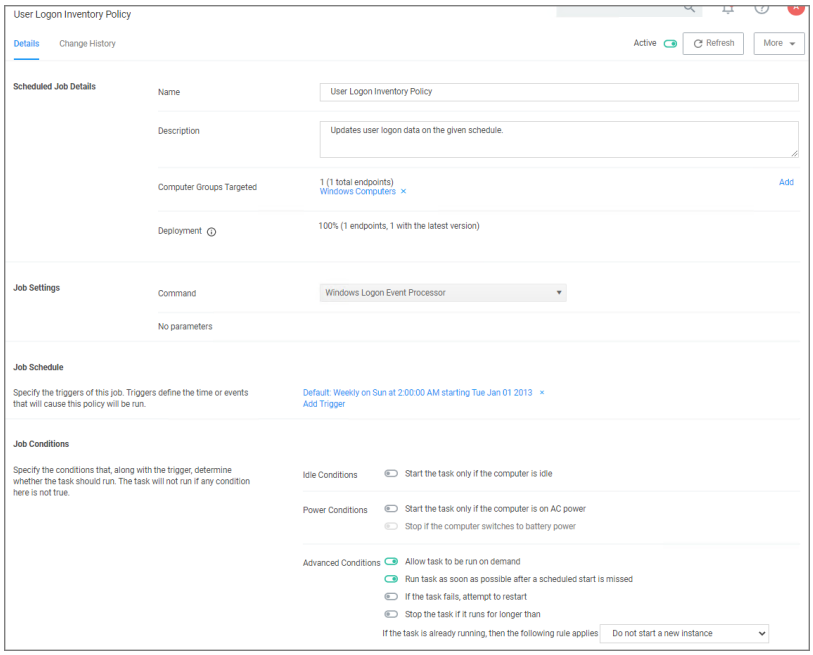
Notice that the unmanaged local user (Harry Otter) defaults to **Remove if found** if **All Other Users and Groups** are set to **Remove if found**.



Logon User Tracking

The Delinea Local Security Agent collects logon and logoff events from Windows on a schedule configured via the User Logon Inventory policy. The Agent collects logon and logoff events and reports them as inventory data. The **Update Primary User for Collection** task calculates the primary user and the primary user and associated inventory data can then be viewed in the Resource Explorer.

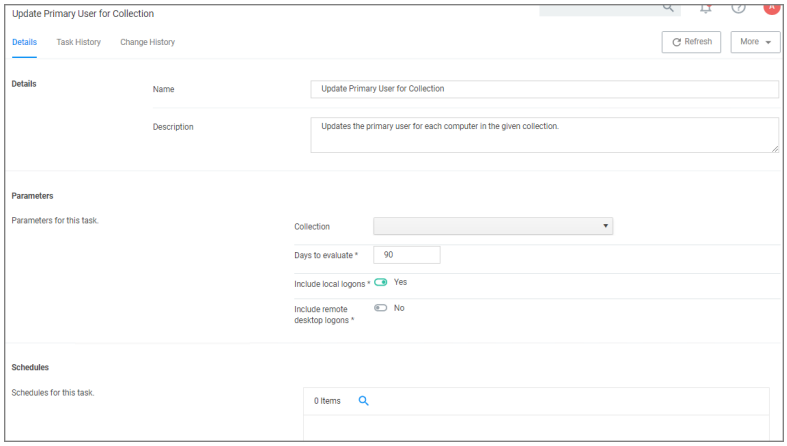
The **User Logon Inventory Policy** is by default active.



If you wish to customize the schedule or any other policy specification, create a copy of the default policy (More > Duplicate) and edit the settings.

The default update primary user for collection task calculates the primary user on a schedule from inventory data.

1. Navigate to **Admin | Tasks**.
2. In the folder tree open **Server Tasks | Local Security** and search for **Update Primary User for Collection**.
3. Click **View**.
4. Customize the settings and schedule by editing the task.

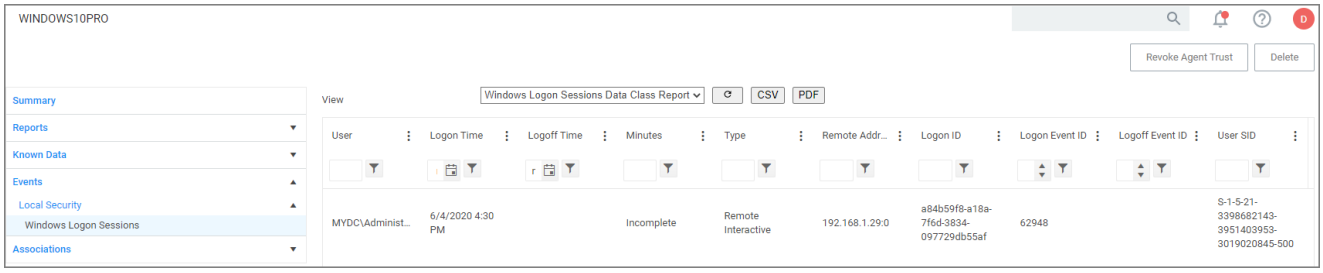


5. Click **Save Changes**.

You can run the **Update Primary User for Collection** task at any time to immediately recalculate the primary user for all computers in the selected collection.

Viewing the Resource

The Windows Logon Session events can be viewed by opening the **Local User/Group Summary** report and selecting a computer resource from the list. Then select Events | Local Security | Windows Logon Sessions.



User Management

The Users page listed under your Computer Group shows a list of local users that exist within this Computer Group.

The User Management and Group Management pages have been configured to load faster by showing the list of managed and built-in users and groups only. Inventoried users and groups will no longer appear by default unless

there are less than 200 workstations in that computer group. You can still manage any group or user on those workstations by clicking **Create User** or **Create Group** available in the top right of their respective tables.

Note: If you need to modify any items within Privilege Manager, duplicate the item and modify the duplicate instead of the built-in item so that an upgrade does not overwrite it.

The information highlighted by the User Management table includes:

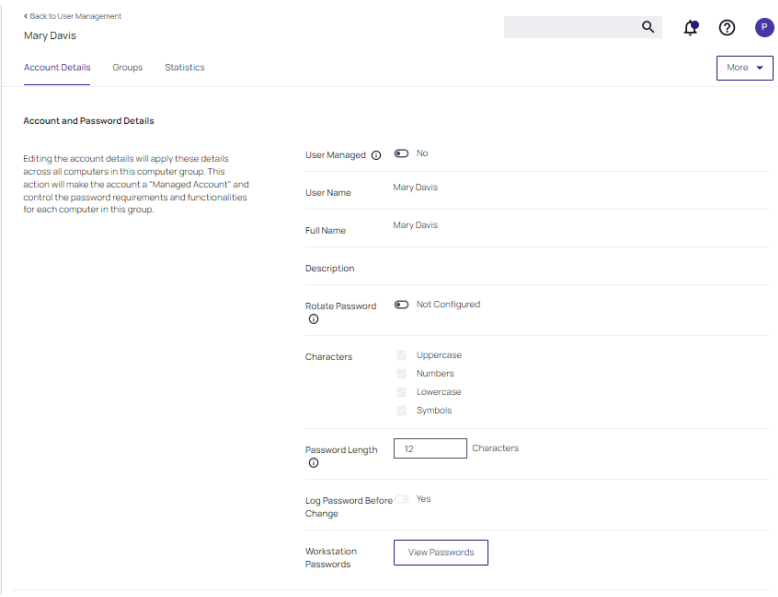
- how many groups each user account is a member of,
- whether the user account was built-in or user-defined, and
- whether or not the account itself is managed.

Local Security allows administrators to manage users and also to manage passwords and password rotation. Managing local users in Local Security means that you are setting a password for the account and can rotate the password as desired.

Creating New Local User Account

To create a new local user,

1. Navigate to your Computer Group for this new user and select User Management.
2. On the User Management page, click **Create User**.
3. Enter the new User Name.
4. Click **Create**.
5. This takes you to the Account Details tab of your new user's account. To create a user through Local Security, it must be a managed user.

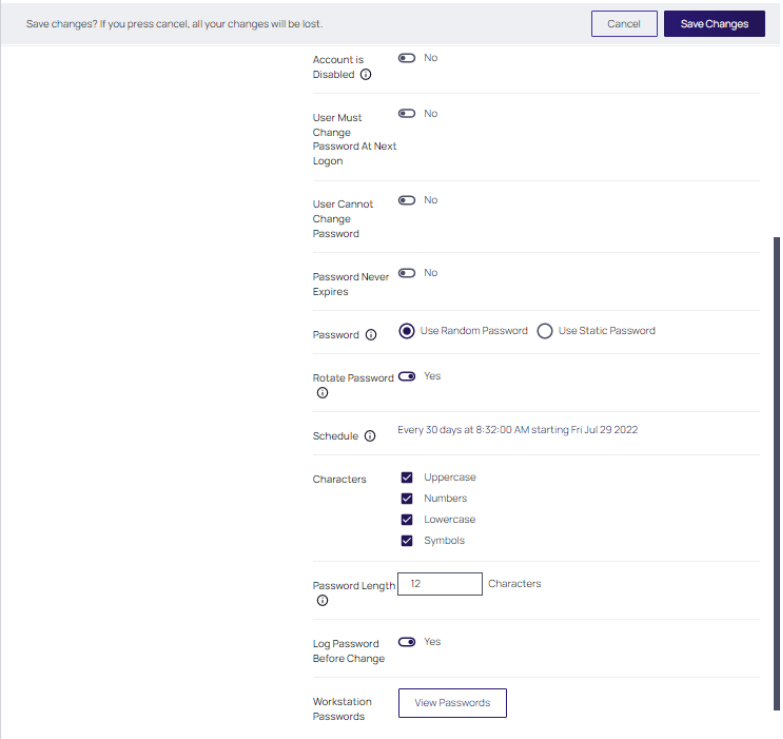


6. Set the **User Managed** switch to **Yes**.

   In Local Security, the most important thing to know about your user accounts is whether or not each is being managed. Managing a local user account means that you are able to rotate the account's password from Local Security's console in Privilege Manager.

   If the password is being rotated, the update schedule determines when the new password is applied.

   Note: The user does not need to be managed in order to rotate the password on a local account.



Note: The following settings are all specific to Windows endpoints and will not be displayed for macOS based Computer Groups:

- Account is Disabled
- User Must Change Password At Next Logon
- User Cannot Change Password
- Password Never Expires

7. Managed user accounts require an initial password when created.

   When the agent first receives the instructions for this account, it will create the account if necessary. Next, the agent sets the password to either the fixed password or random password, depending on which option is selected. This occurs regardless of whether the user existed or not. This overwrites any existing password.

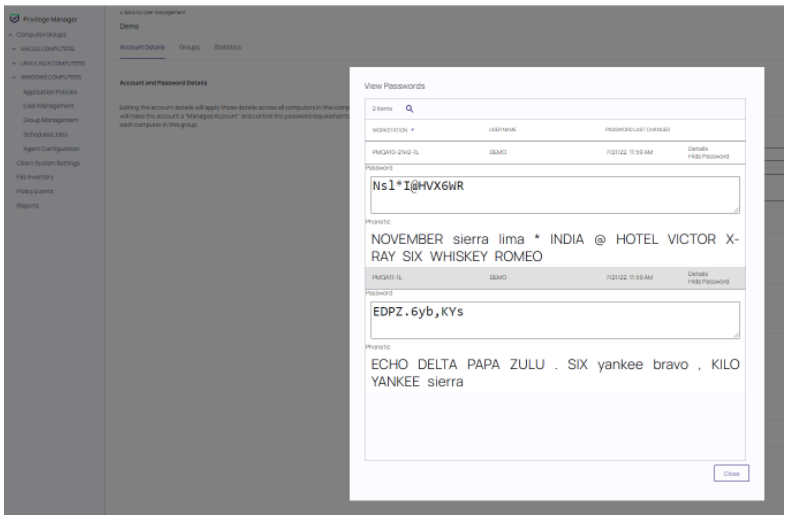
   Note: If the user account is enabled, disabled, or deleted, it will repeat this initial deployment process.

   In an addition to creating a static initial password, an additional option to create a randomized initial password is available.

   If **Use Static Password** is selected, click the **Edit** link and specify a password, according to the password criteria set. The user will be able to login to any computer defined for the user account using this password. The password becomes effective at the point that the User Management task is updated on the agent endpoint (a message will be returned to the server).

If **Use Random Password** is selected, a different randomized password will be produced for every agent endpoint workstation that the user is managed on. Random passwords are also based on the password criteria set. The password(s) generated will display when the **View Password** button is selected, but only after the User Management task is updated on the agent endpoint (a message will be returned to the server).

For example:

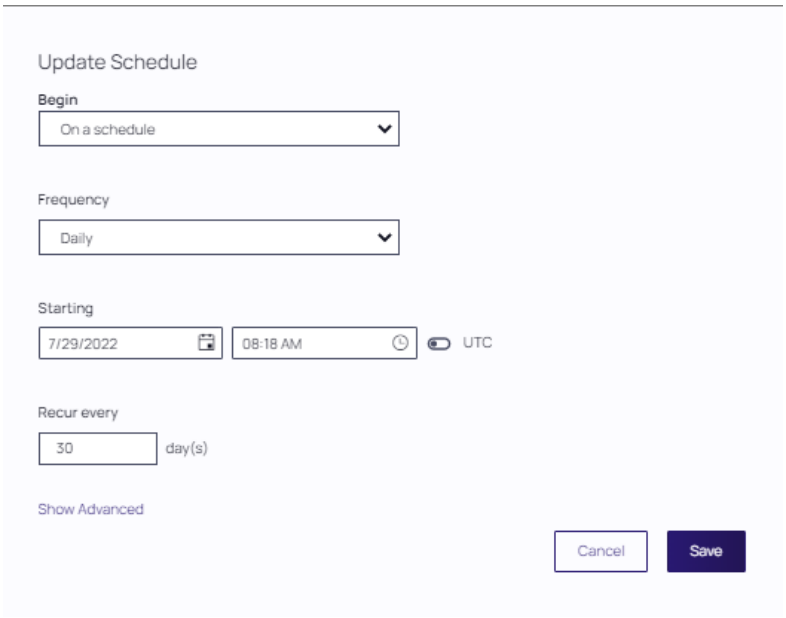


Select the method for password creation (Static or Random), then edit **Characters** and **Password Length** settings pertaining to the user's password.

8. Managing users, passwords, and rotation schedules often go hand-in-hand, but not every managed user account also requires password rotation. For example, service accounts are managed, but usually do not have password rotation setup. Password rotation can also be setup for existing users without having to provision user accounts.

   Note: Password rotation is an option that is not required for all accounts, especially not for service accounts.

   If password rotation is desired, enable **Rotate Password**. When prompted, click **Confirm Manage Password**. Click the link provided in the **Schedule** field and supply values in the **Update Schedule** dialog box and click **Save**. The password on this account will be rotated based on the Update Schedule details.



9. When all account settings are satisfactory, click **Save Changes**.

Editing a Local User Account

While editing a user, you can change the account User Name, add details like the full name of the user, disable the account, or update the schedule that pushes out modifications to endpoints.

The **Groups tab** for a Local Account tells you how many groups and computers the account is on. Clicking on a Group Name from this page directs you back to the details of that local group.

The **Statistics tab** for a local user account highlights some quick visual statistics and links to relevant reports based on key factors, like how many computers from your network have this user account and whether there have been changes made to the user's membership within the specified period. Click on the graphs to drill down into more details.

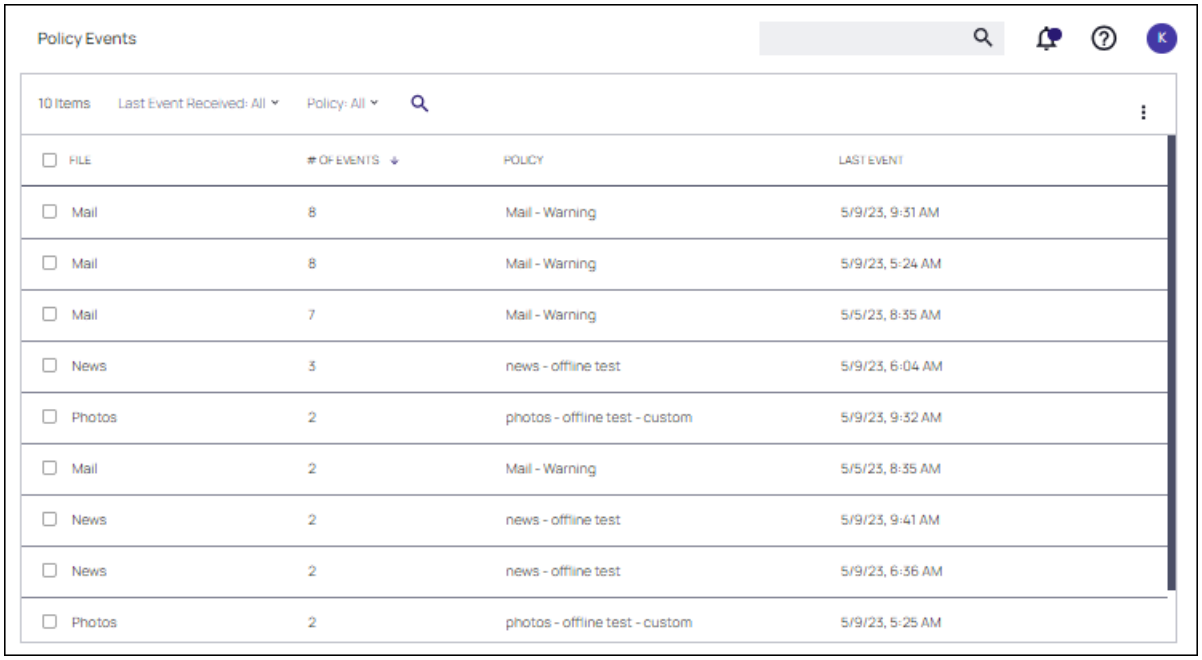
Reports Relating to Managed Accounts

- **All Computers with Managed Passwords**: Lists all computers that have at least one local user with a managed password.
- **Password Disclosure History**: Lists all local and provisioned user's passwords that have been disclosed in a given time frame.
- **Disclosure Summary (Local User)**: Lists all local users whose managed password has been disclosed in the given time frame.

Policy Events

Application control events or **Policy Events** are created if you choose to have one or more policies send feedback (from the endpoint to the server) each time the policy is triggered.

Under **Policy Events** Privilege Manager provides access to all information collected and events discovered due to using monitoring policies with the **Audit Policy Events** switch set to active.



Event Details

Select an event or multiple events. Details are displayed in a panel on the right. The details provided are the application or process name that triggered the event and based on which policy the event was recorded, including a short policy description. You can also see how often this event has occurred.

Policy Event Actions

The buttons in the lower right of the page allow you to apply policy event actions for the policy.
The check boxes provided allow you to select multiple events (or all events). Use the **FILE** check box to select all events, or to deselect the current selections.

Note: Only the **Acknowledge All** action can be applied to multiple policy event selections.

Create Filter

Use the details view to either create a filter or view the file. If you choose to **Create Filter**, you can also select to immediately add that filter to an existing policy.

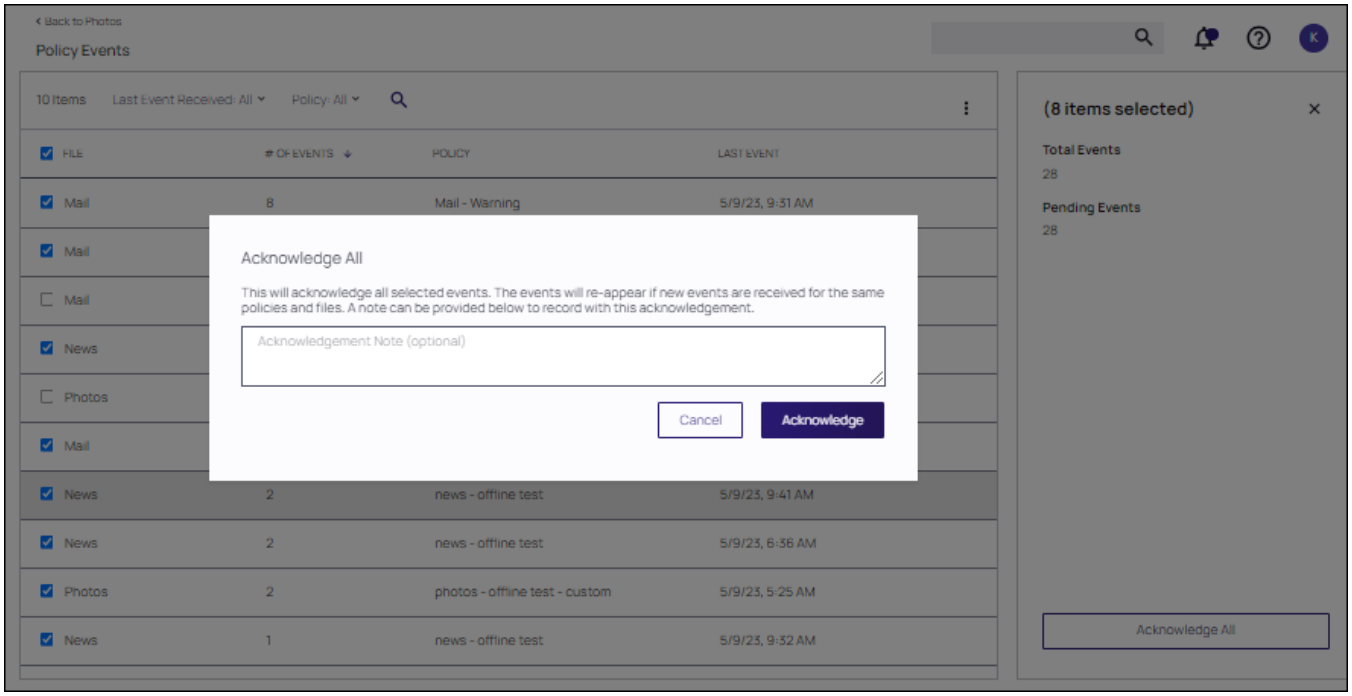
View File

If you choose **View File**, you can drill into the event details further. Refer to Events Drilldown.

Acknowledge All

If you enabled the **Show Acknowledge Events** switch, **Acknowledge Events** is visible. Refer to Privilege Manger Solution for details.

Enable the check boxes for the events to be acknowledged, then click **Acknowledge All**. Supply a note for the acknowledgment and click **Acknowledge**. The selected events are removed.



Change Filter Criteria

Click the ellipsis in the top right of the Policy Events list to **Change Filter Criteria**.

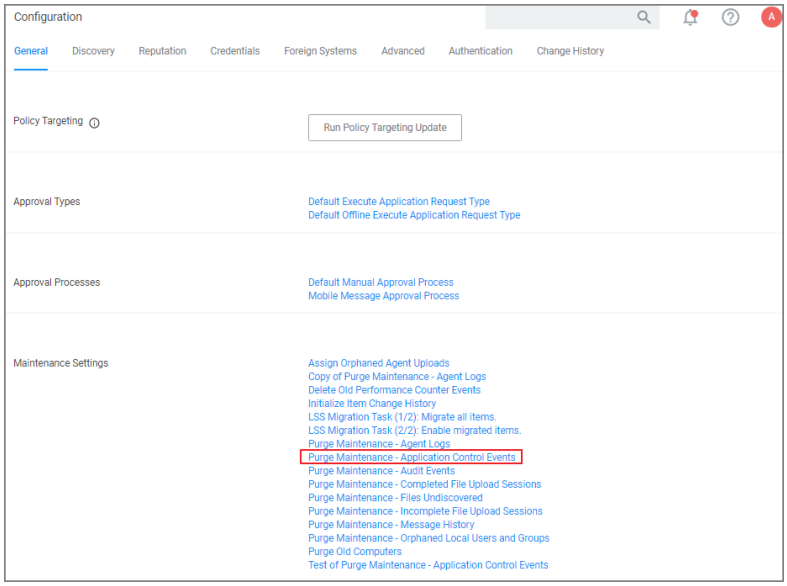
Events Maintenance

In Privilege Manager versions prior to 10.6, all events are stored unless **manually purged**. Event storage uses database space and can impact performance of dashboard queries so it is sometimes desirable to purge the stored events.

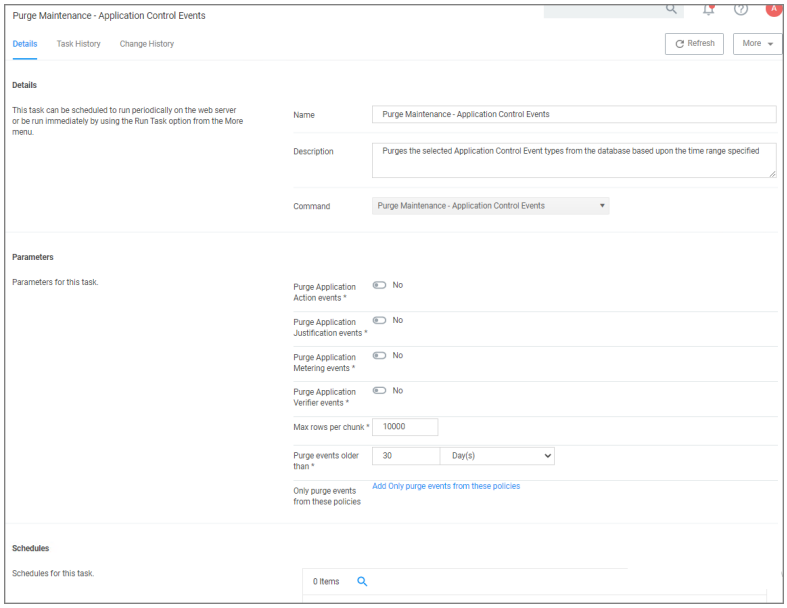
Privilege Manager version 10.6 and up, includes an option to specify the **maximum number of events** to be stored (rather than let the system continue to add events to be stored until manually purged).

Manually Purge Events

1. Navigate to **Admin | Configuration** and select the **General** tab



2. In the **Maintenance Settings** section of this page, click on **Purge Maintenance - Application Control Events**.

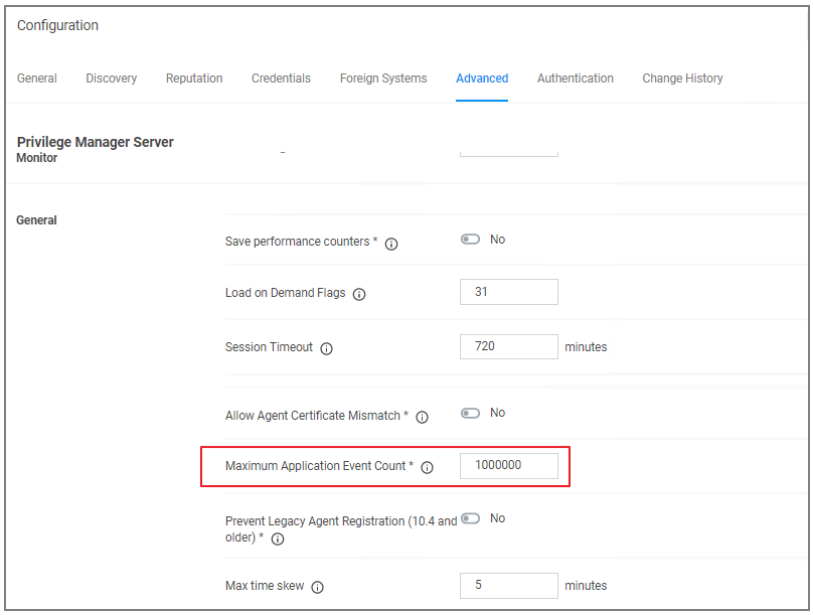


The Description text explains what this feature does: "Purges the selected Application Control Event types from the database based upon the time range specified".

3. Under **Parameters**, set the switches and edit values based on how you want the maintenance to be performed for your instance.
4. Click **Save Changes**.

Maximum Event Count: Basics

1. Navigate to **Admin | Configuration** and select the **Advanced** tab.



The "Privilege Manager Server" section of the page shows the option "Maximum Application Event Count" and its default value, which is 1,000,000.

You can change the value, but storing a large number of events could cause database issues and slow down dashboard queries. Save your changes, if you edit the number.

Note: In the Cloud version of Privilege Manager, the Maximum Event Count cannot be changed by the user; it is fixed at its default value.

Maximum Event Count: Additional Information

The points below provide additional information about the Maximum Event Count:

- The count value is a total for all policies; it is not a per policy setting.
- The count is treated as a rolling window; if a new event would cause the count to exceed the maximum limit, the oldest event is removed.
- The manual purge, as described in a previous section, is still available.
- As mentioned in the previous section, the Maximum Event Count cannot be changed by the user in the Cloud version of Privilege Manager; there it is fixed at its default value.

Best Practice: Policy Feedback

In Privilege Manager, the option to Send Policy Feedback is the main notification mechanism about application installation and execution on user endpoints. Using Send Policy Feedback is recommended while systems are in Event Discovery and Learning Mode. This helps administrators to gather data, analyze patterns, and then assign actions to application events retrospectively.

It is not recommended to use Event Discovery for all configurable options and all user endpoints all the time. Event Discovery in an established production environment should be targeted to not generate unnecessary and overwhelming amounts of data.

Privilege Manager isn't a SIEM tool, so it shouldn't be capturing events from every endpoint. On the Conditions tab of any policy, users can see what is being targeted. The Application Filters on the policies are typically built with the target file name (and with established naming conventions, the policies and filters are easier to filter and to determine what they are targeting). The Privilege Manager User role can be assigned to the employees who need to audit these policies. That role will give them the ability to read items in Privilege Manager but not make any changes. Those users, as needed, look at the policies to see what's being targeted and can then relay that information to administrators that need to know those details.

Privilege Manager should not be used to audit events on all endpoints, but small scope audit can be done. For those, an elevate policy can be copied and targeted to a specific user, machine, or very small group with send policy feedback. As long as it's a small sample, it shouldn't flood the database with events. This type of audit policy can be assigned to an AD group. Change what user or machine is in that group to change who/what is spot audited. It provides a small example of what is being elevated.

What's First

Privilege Manager includes policies to discover when an end user runs an application that requires administrative rights. Creating policies for any known applications and tasks should be first. Organizations are aware of applications that require elevated permissions to run or install. Collect any files that have already been identified and create policies targeting those applications.

Often different users have different rights on their endpoints, based by division, hierarchy, or other classifications. Privilege Manager can quickly inventory local groups and users. If current permissions are unknown, use Privilege Manager to discover which accounts have administrative permissions on each endpoint. Action can be taken to immediately remove suspicious or unwanted users and groups.

Understanding which users and groups have administrative rights, allows you to properly assess what permissions should exist on an endpoint.

Note: Do not elect to Send Policy Feedback for trusted applications for those specified groups that are cleared to use and install the applications.

Event Discovery

Event Discovery is Privilege Manager's process to determine which applications will require policies.

Based on your use cases, different Event Discovery policies should be enabled. Enable event discovery for the most common use cases like:

- applications that require elevated rights,
- installers, and
- processes that trigger a UAC prompt.

Privilege Manager admins will work through the results of Event Discovery and build policies targeting these applications. Admins will determine if a file should be added to an allow, deny, or elevation policy. If elevated, determine if the file will be silently elevated or if justification, approval, or another workflow will be required.

Add the applications that are discovered to policies with priorities to be triggered before Event Discovery. This will prevent those applications from continuing to be discovered by Event Discovery in the future.

Following this process will naturally clean up the results from Event Discovery.

Refer to Discovery in the Admin menu section.

Never Disable Event Discovery

Event Discovery is not a short process. It's an integral part of Privilege Manager. Once Event Discovery is enabled, it is never disabled.

Even after all policies have been built and all end user needs are met and the local admin groups are empty on all endpoints, you'll still want to know if there are new items that require elevated permissions. Or, after admin rights have been removed, you may want to setup Event Discovery to send feedback if someone runs an application in a context that is unexpected and highly suspicious.

What is discovered and who/which machines Event Discovery targets may change, but Event Discovery will always be used in some capacity.

Event Discovery will never be disabled – you will always want to discover new events that require elevated rights. Consider a maturity plan for Event Discovery.

- Begin by silently discovering applications and creating filters/policies.
- As policies are tightened, add a justification prompt for new items.
- When admin rights have been removed and policies are set, use an approval process or reputation check for newly discovered items.

Event Discovery cannot be sped up. Files will only be discovered when end users initiate a process. If a certain team has an application that is only used at the end of the quarter to finalize business, that application will only be discovered once it is run by the end user.

The scale can be adjusted to ensure the workload is manageable. Start small, understand the workload when the pipeline is slow, then scale to the workload that can be maintained.

Purpose of Event Notifications

Event notifications are helpful and important when administrators want to initially establish policies and to continually monitor the installation and execution of new/unknown applications.

For a production environment it is necessary to know when potentially dangerous applications are installed on a user endpoint. It is not important to be notified every time a white listed application is installed or run on a system.

> **Note:** That means that silent elevation policies do not need an event notification and should not have Send Policy Feedback enabled. Information should only be given on application events that require a follow-up with actions.

Approval and justification policies always generate an event as required for an audit trail. These events cannot be subdued.

Self-elevation, deny list, and other events on an endpoint triggering UAC are part of the never-ending event discovery process in an organization.

Best Practices

Create policies that are used for a certain amount of time before they are revisited and potentially adjusted for current needs. Target specific systems or user groups with group specific policies. Once those requirements are set, define what events will need a follow-up action in your environment:

- What exceptions can be made if any
- When to use overrides
- What to block
- What to deny list.

For certain groups of users, it might also be an idea to target a specific machine routinely to use the data to fine-tune any policies that are enforced on the endpoint. Group Management based on existing groupings – AD OUs, AD user groups, SCCM groups, etc.

However, requirements and circumstances are not set in stone and revisiting existing and established policies is part of a best practice approach in PAM.

It is important for administrators to know when (and potentially why) deny listing policies are triggered. It indicates that employees are violating company policy. However, if this happens a lot, it might indicate that there is a business need for this application and that the blocked software was not fully understood.

Examples

Send Policy Feedback

An UAC override policy allows a user to elevate a program not blocked by a deny listing or elevated by an allow list, by reentering their password to install/run, is a good candidate for sending policy feedback. It presents an exception to normal execution of programs as an unprivileged user. This type of event logging should be used to identify new programs to add to silent elevation policies if the frequency warrants, or to audit user usage to elevate items they shouldn't to mark them for blocking or follow up action.

Don't Send Policy Feedback

For most business organizations, it makes no sense to implement a policy that sends feedback when a MS Office product or the company wide instant messaging product is installed or run. For user groups like developers, programming tools are needed and running those should not trigger any notifications.

Events Drilldown

After selecting **View File** the Summary page is displayed for the process that triggered the application policy event. The summary page lists details, such as the File Name, Original File Name, Product Name, Version, Internal Name, Company Name, Copyright, File Hashes, and provides the ability to view reputation details if reputation checking is enabled.

When drilling down into this information the context determines the information that is provided:

Event/Application Context	Resource Context
top level	drilldown options

Event/Application Context | Resource Context

chrome.exe

Summary

Reports

Computer Locations

Policy Events

Similar Files Report

Observed Parent Pro

Known Data

File Details

File Digital Signature

File Inventory

COFF Header

File Digital Signatur

File Header Raw

macOS Package Su

Hash

Software Manageme

Manifest

Version Info Raw

Win32 Executable

Events

Infrastructure

Resource Discovery

Associations

‹ Back to chrome.exe

computer

Summary

Reports

Policies on Endpoint

License Reservations

Task History

Computer Group Membership

Known Data

Basic Inventory

Win32 Computer System

Win32 Computer System Product

Win32 Operating System

File Inventory

File Location

Global Identity

Infrastructure

Agent

Server Node

Local Security

Local Account Settings

Security Management

Global Domain Details

Software Management

Shared Folder Settings

Windows Service Settings

Reports

Computer Locations

The **Computer Locations** report lists the computer name, domain, operating system, and file path information for the recorded policy event. Clicking on a computer name listed, opens that computer's (end point's) summary page, with the options to further drilldown into details contextual to that specific computer.

Policy Events

The **Policy Events** report lists all event policies that were triggered by the event. Clicking on items in this list drills into the process details.

Similar Files Report

The **Similar Files Report** lists all files that are similar to the recorded policy event.

Observed Parent Processes

The **Observed Parent Processes** report lists all parent processes for the recorded policy events. This report allows the view of all parent and grant parent processes as recorded.

Known Data

Known Data Provides all the discovered details about the application triggering the event.

File Details

File details lists information like extension, size and if the file is protected or not.

File Digital Signatures

File digital signatures provides information about the signer, countersigner, and timestamp of the file signature.

File Inventory

File inventory provides information about the following details:

- Coff Header
- File Digital Signature Raw
- File Header Raw
- macOS Package Summary

Hash

Hash lists the hash names in use and provides the hash and hex hash values.

Software Management

Software management provides information about the following details:

- Manifest
- Version Info Raw
- Win32 Executable

Events

Infrastructure

Infrastructure provides information about the following details:

- Resource Discovery

Associations

Associations are usually only available on a resource context level.

Details as they Pertain to the Selected Resource Context Level

The summary page provides the computer name, created and modified dates, offers a switch to turn on monitoring of the resource to generate alert notifications about certain actions performed by the resource, and it provides a Health status for the endpoint, like the policy and registration states, and if the resource is managed.

Reports

- Policies on Endpoints: Lists the policy names of all the policies on the endpoint. Information provided:
  - Has a Version of the Policy: True/False indicator
  - Has Current Version of the Policy: True/False indicator
  - Policy Last Modified: Date of last policy change.
  - Policy Applied to Agent: The date when the policy was first applied to the agent.
  - Agent Last Received Policies: The date the agent last received policy updates.
- License Reservations: Lists all the licenses that apply to the endpoint including the reservation date.
- Task History: Lists all the tasks run and completed including status details for the endpoint.
- Computer Group Membership: Lists all the computer groups this computer is a member of.

Known Data

- Basic Inventory: Provides information pertaining to the local system data, including OS.
- File Inventory: Provided information about the application/process names and their file path as well as discovery date.
- Global Identity: List the domain and user id information.
- Infrastructure:

  - Agent: Lists the agents on the endpoint and provides version details.
  - Server Node: Provides information about the server heartbeat and version.
- Local Security: Provides local account setting information.
- Security Management: Provides Global Domain Details.
- Software Management:
  - Shared Folder Settings: Lists the shared folders, their path, maximum users, if they are secured or not, provides remarks about the type of share.
  - Windows Service Settings: Lists all Windows services, the primary and secondary file names, user account, start and service types.

Events

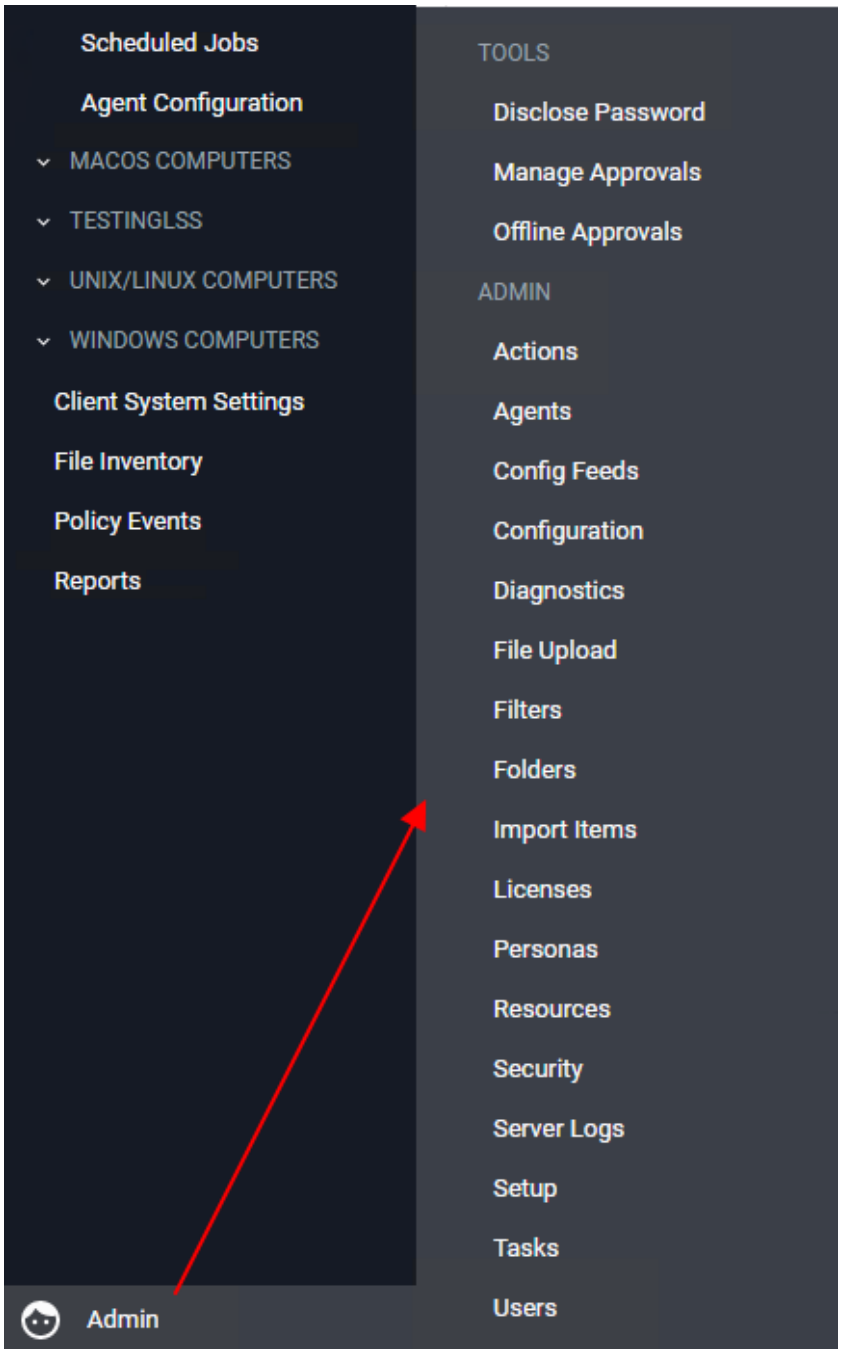
- Application Control
  - Application Action: Lists all application file names, the policy names, the user, file path, event received details, and information about the command line executed to trigger the event.
- Local Security
  - Windows Logon Sessions: Lists all the user logon/logoff events with details about duration, type, ID User SID to just name a few.

Associations

- Computer Primary User: Provides the name of the primary user on the managed endpoint.
- Computer Local Group: Lists the names of the local user groups on the endpoint.
- Computer Local User: List the name of the local user.

Administration

Access to many system administration tasks happens via the **Admin** menu at the bottom of the left navigation menu.



This section of the Privilege Manager documentation covers how to setup and configure resources listed under the Admin Menu. There are other common tasks an Administrator will do like create, edit, and delete policies, local groups and users, those are detailed further under their respective sections and are not addressed here under Admin procedures.

Best Practices

Note: If you need to modify any items within Privilege Manager, duplicate the item and modify the duplicate instead of the built-in item so that an upgrade does not overwrite it.

The following topics are available:

- Using a Service Account to run the IIS App pool
- Prevent Read and Write Access to File Types or Locations
- Securing the IIS Server
- Updating to higher security algorithms

Security Algorithms

Privilege Manager v11.1 introduced configurable security algorithms.

Configuration of security algorithms is managed via **Admin | Configuration | Advanced** under the Agent section. Refer to "Advanced Tab" on page 559.

Delinea recommends that all customers update to SHA256 at this point.

Server-Targeted Settings

The following settings are targeted at the Privilege Manager server.

Allowed agent event signature algorithms

This setting specifies what signature algorithms the server accepts when processing events from the agent. The new minimum standard for agents v11.1 events is XML RSA/SHA256. XML RSA/SHA1 is considered legacy support for older agent version only.

By default in v11.1 and up XML RSA/SHA256 and SHA1 are configured. Once your server only communicates with the latest agent version and all your policies/filters have been updated, SHA1 can be removed from the configuration.

Client item signature algorithms

This is the list of one or more signature algorithms the server will use when signing client items.

- **Legacy Value**: XML RSA/SHA1
- **Default**: Both XML RSA/SHA1 and XML RSA/SHA256.

Allowed client item signature algorithms

This setting specifies the signature algorithm(s) on tokens the server should accept for agent service calls.

Agent-Targeted Settings

These are settings that are targeted at agents, and will be part of agent configuration items. If the settings are not specified in the agent configuration contract XML, then the global setting will be sent to the agent.

Agent Event Signature Algorithm

This is the signature algorithm agents are instructed to use when signing XML events.

- **Legacy/unspecified**: The legacy value is XML RSA/SHA1. Agents should continue using this if not specified in their configuration.
- **Default**: XML RSA/SHA256

Inventory Hash Algorithms

These are the hash algorithms that agents should use when reporting inventory for resources.

> **Note:** The agent should always report as many hashes as possible from the configured set. Legacy hashes don't do any harm except maybe take up a bit of space.

- **Legacy**: The legacy values are mixed, some resources (like Folders) were using MD5, most files and other resources used SHA1.
- **Unset**: If the agent doesn't have a configuration value for this, it reports all hashes it can from the set of (MD5, SHA1, SHA256, Authenticode, Authenticode 2).
- **Default**: MD5, SHA1, SHA256, Authenticode, and Authenticode2.

> **Note:** Authenticode is a Windows technology for signing executables, it essentially contains the hash of the raw executable before signing. For non-Windows OSes and non-Executable resources, this hash is ignored.

Prevent Read and Write Access to File Types or Locations

You can restrict access to specific file types or locations using Privilege Manager. To prevent read / write access to file types or locations, do the following steps:

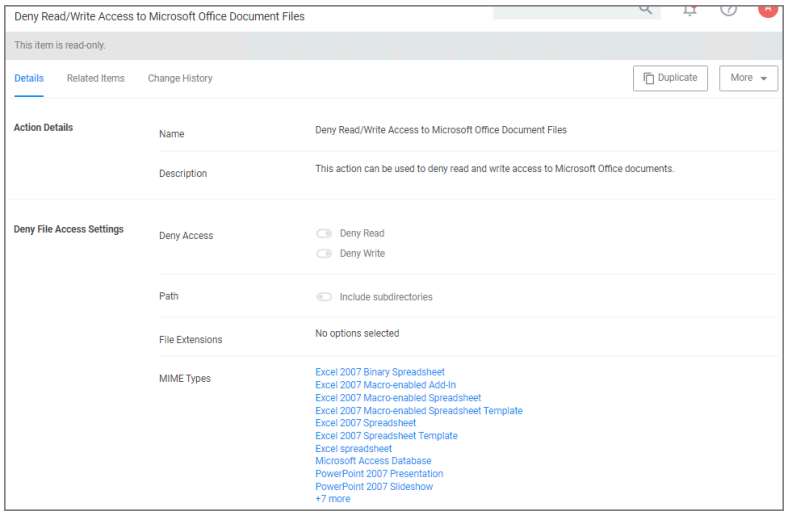
- Create a Deny File Access Action
- Create an Application Control Policy to which you will add the Deny File Access Action
- Test the privilege reduction you've just created

In the following scenario you will create a Microsoft Word document and save it on your machine to:

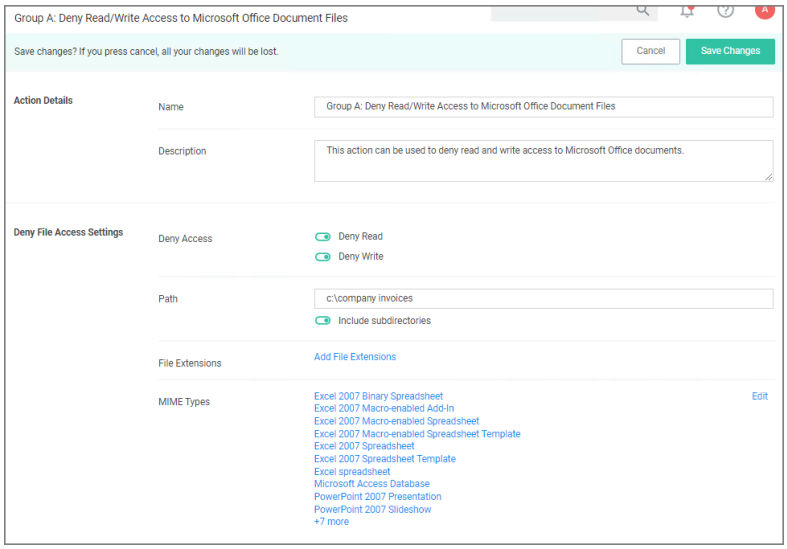
```
c:\company invoices\invoice 101.doc
```

Create a Deny File Access Action

1. Navigate to **Admin | Actions**.
2. Search for **Deny File Access Action**.
3. Click on **Deny Read/Write Access to Microsoft Office Document Files**.



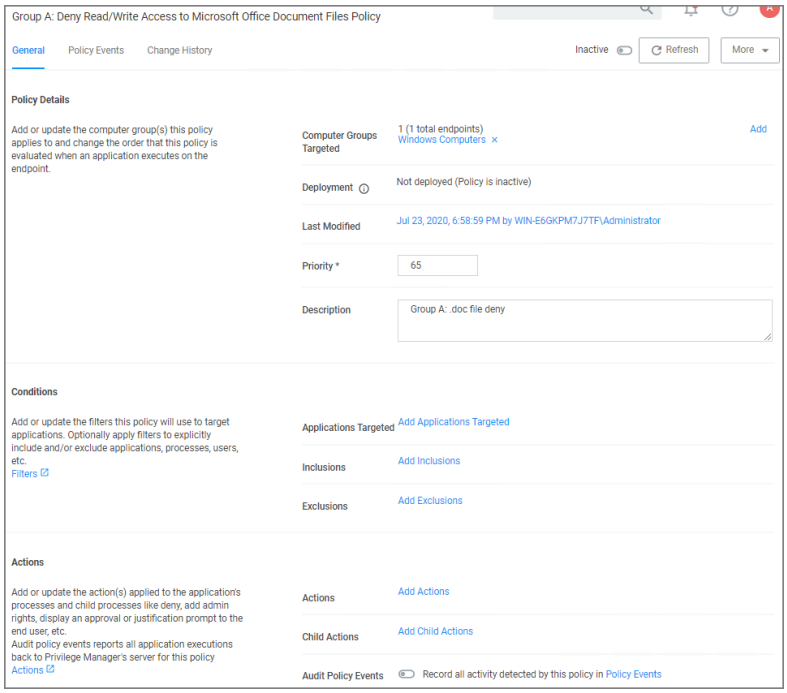
4. Click on **Duplicate**.
5. Name the new copy of the action and click **Create**.
6. Enter the path of the file location (`e.g., c:\company invoices`), for our example we also set the switch to include subdirectories.



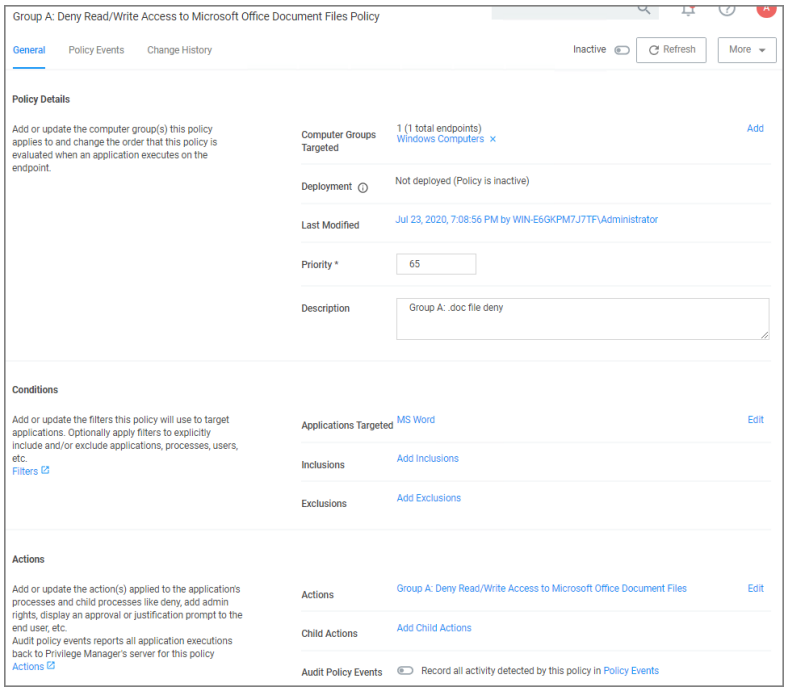
7. Click **Save Changes**.

Create an Application Control Policy

1. Under your Computer Group select **Application Policies**.
2. Click **Create Policy**.
3. Select **Skip the wizard, take me to a blank policy**.
4. Add Name and Description, click **Create Policy**.



5. Under **Conditions | Applications Targeted**, click **Add Application Targeted**.
6. Search for **word** and add the **MS Word** filter.
7. Click **Update**.
8. Under **Actions**, click **Add Actions**.
9. Search for and add your **Deny Read/Write Access to Microsoft Office Document Files** Action.
10. Click **Update**.



11. Click **Save Changes**.
12. Set the Inactive switch to **Active**.
13. Next to Deployment, click the **i** icon and run the **Resource and Collection Targeting Update**. After you run update, the appropriate endpoints will receive the new policy.

Test Access

Verify that the restricted access you set up was successful by applying the following tests:

- In Microsoft Word, open `C:\company invoices\invoice 101.doc`. The file is read only and can't be modified.
- Create a new document and attempt to save it to `c:\company invoices\`. You will be unable to open it and will receive a File Permission error.
- Verify that you can create or modify a Word document in a different directory.
- In Microsoft Excel, save a spreadsheet to `c:\company invoices\invoice 101.doc`. The permissions are limited to Microsoft Word.

Using a Service Account to run the IIS App pool

Delinea recommends setting up a domain service account that can both:

- access the Delinea product's SQL database
- run the IIS Application Pool(s) dedicated to your Delinea product

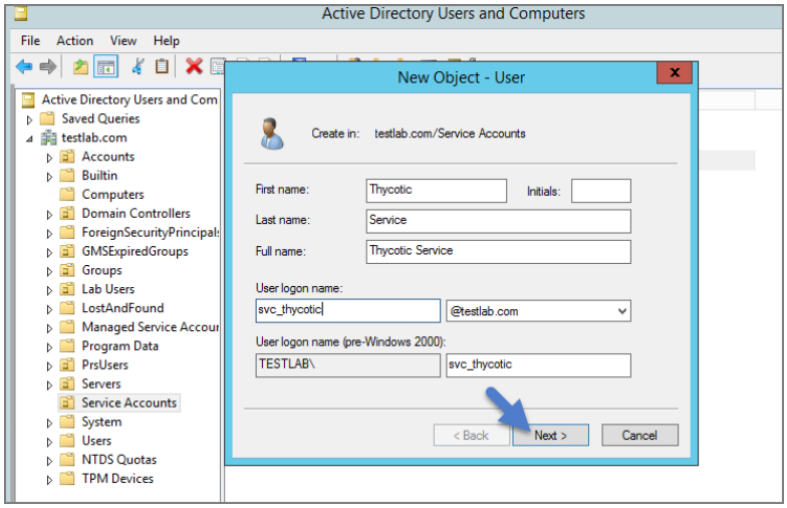
> **Note:** The service account created in this KB should NOT be the same account that is created during the installation of SQL and used to manage SQL as a whole.

To set up this service account correctly you will need to:

1. Create a service account in Active Directory that will be dedicated to your Delinea product (Domain).
2. Grant the service account access to the SQL Server database (Database).
3. Assign the service account as Identity of the Application Pool(s) in IIS (Web).
4. Grant folder permissions for the service account on two folders (Web).
5. Configure User Rights Assignment to the service account (Domain AND/OR Web).

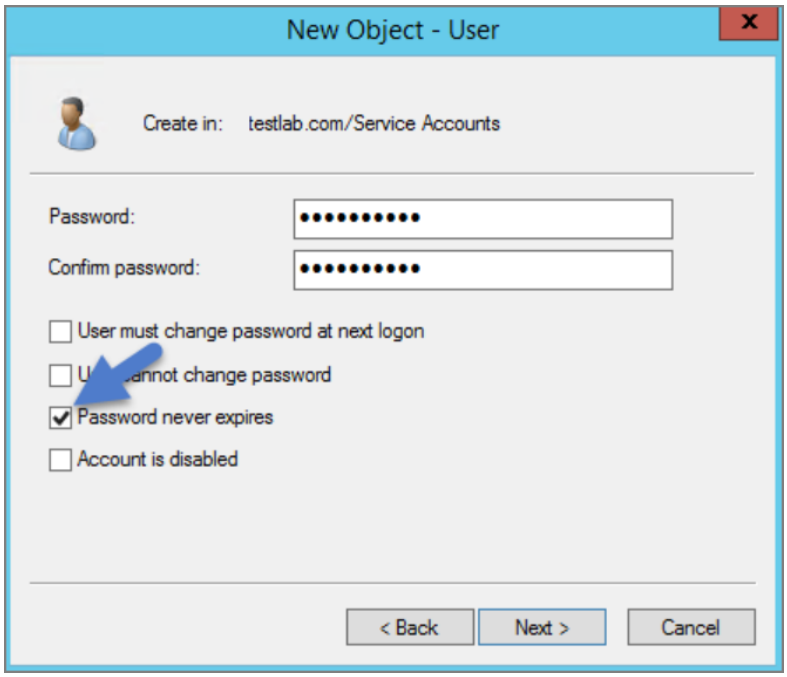
Creating a Domain Service Account

1. Open the **Active Directory Users and Computers** link from Administrative Tools.
2. Right-click the directory where you want to assign this account (i.e., testlab.com > Service Accounts).
3. Click **New** and **User**.
4. Add a name and logon name for the service account.
5. Click **Next**.



6. Enter a password.

> **Note:** Uncheck "User must change password at next login if checked." Check Password never expires or the account could lock you out of Privilege Manager.

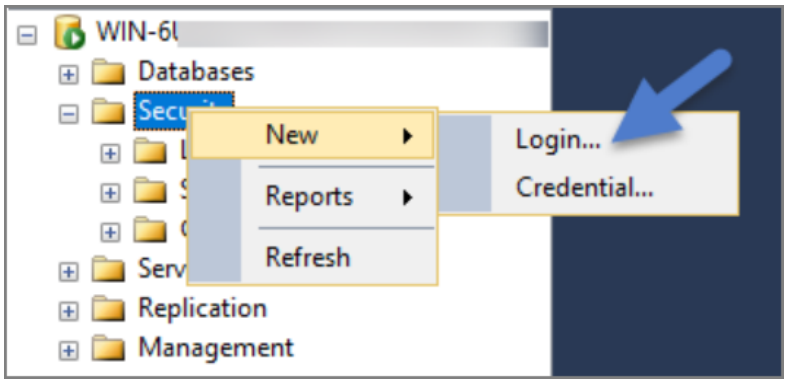


7. Click **Next**.
8. Click **Finish**. This account can now be given access to the database server and the application server.

Granting Access to SQL Database

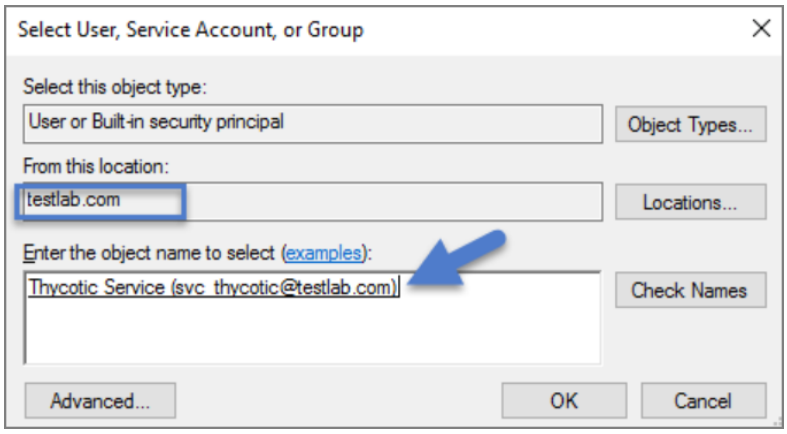
You must have SQL installed on your database server before completing these steps:

1. Using SQL Management Studio (on your database server), connect to your Delinea product's SQL Database using an Administrator account.
2. Right-click on the Security node (Ensure this is the top most Security node under the instance and not under the database name itself).
3. Click **New** and **Login**.

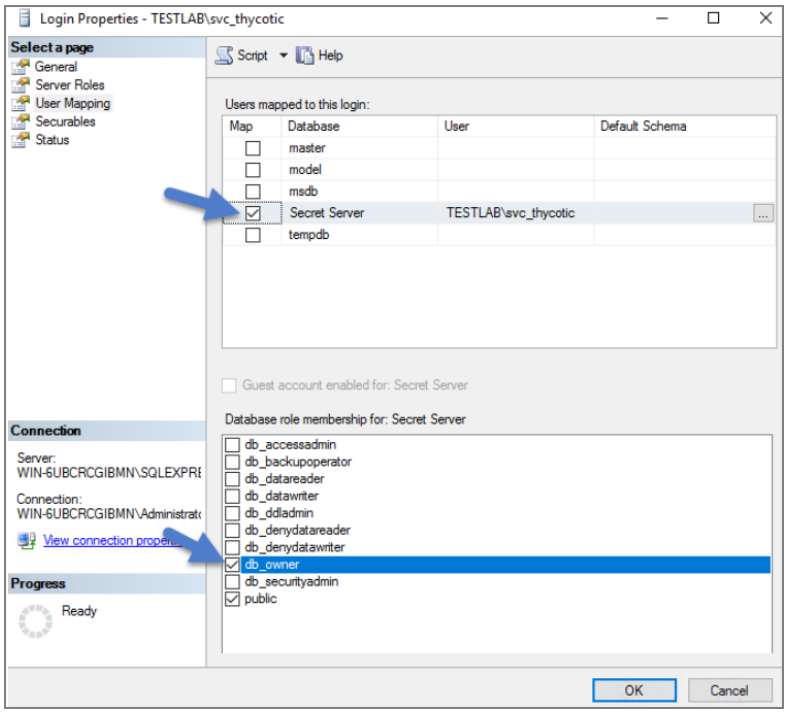


4. Ensure Windows Authentication radio button is selected.
5. On the New Login page click Search... Ensure that your domain/AD server is selected as the location.

6. In the “Enter the object name to select” box enter the Login name created for your Delinea service account (e.g., “svc_thycotic”). Click Check Names and select the correct account.
7. Click **OK**.

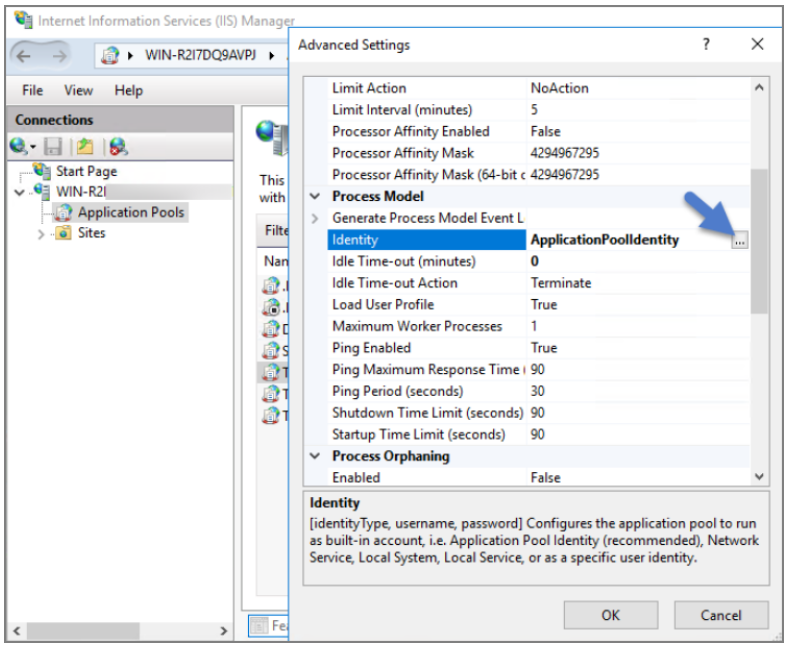


8. If you have already created the database for your Delinea product, under User Mappings select the database and check the box to grant the db_owner permission (example pictured below). OR - If you have not yet created the Database, Under Server Roles select db_creator
9. Click **OK**.



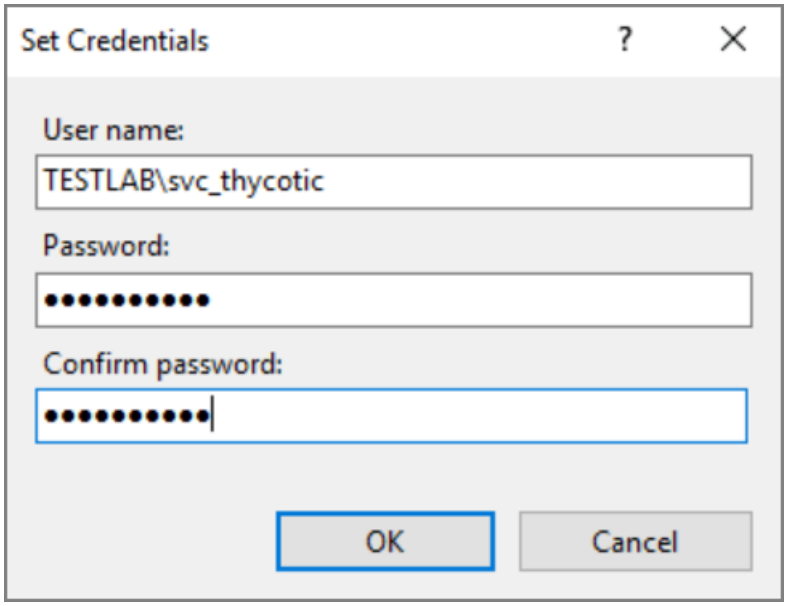
Assigning Identity of Application Pool(s) in IIS

1. Open IIS on your web server **Search | inetmgr**.
2. Locate the application pool(s) that your Delinea product is using, right-click Advanced Settings.
3. The Identity box in the **Process Model** section, click the three dots on the right of the box.



4. Select the Custom Account radio button.
5. Click **Set** and enter your service account's name and password.
6. Click **OK**.

Note: You will need to perform this step for multiple application pools for Privilege Manager.



Granting Folder Permissions

You must have the Delinea product application files installed (on your web server) before completing this section.

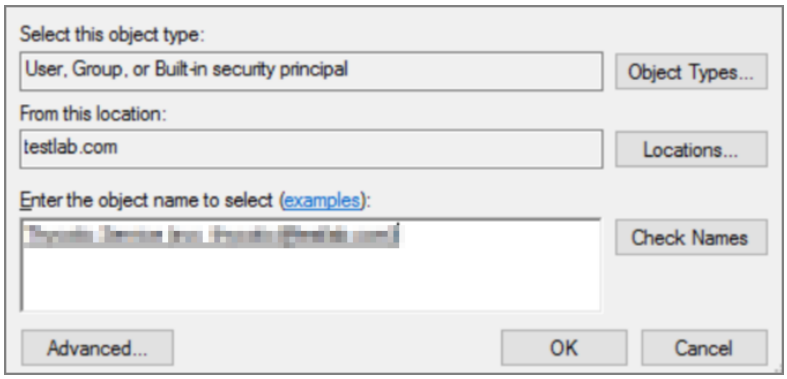
Following the steps below you will need to give the service account **Modify** access to two folders:

- **C:\Windows\TEMP**
- The folder where your Delinea product's application files are located

  (i.e., **C:\inetpub\wwwroot\SecretServer**)

You must have the Delinea Product Application Files installed on your web server before completing these steps.

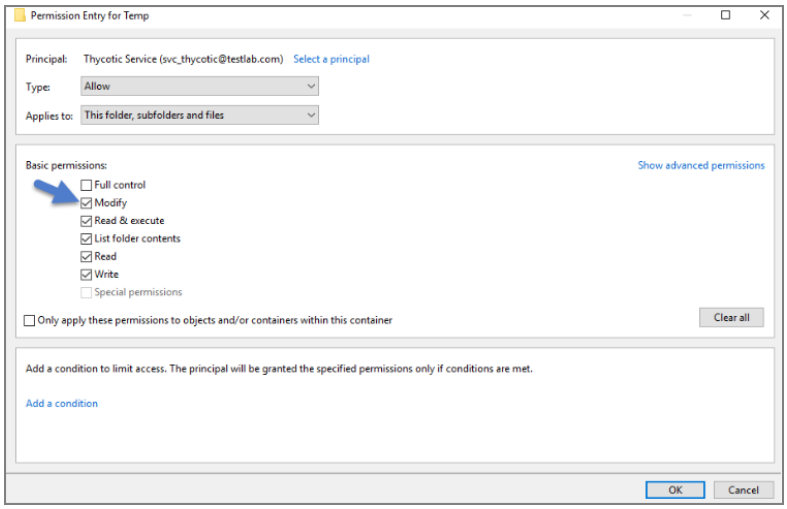
1. Open **C:\inetpub\wwwroot\TMS** and right-click the folder you are modifying.
2. Click **Properties** | **Security** | **Advanced**.
3. Click **Add** and then select a principal.
4. Ensure the domain machine is listed as the Location and type the service account under the “Enter the object name to select” box, click Check Names and Enter network credentials for accessing your domain machine.
5. Click **OK**.



6. Click the **Modify** checkbox.

   Your service account should now have Modify, Read & execute, List folder contents, Read, and Write permissions for this folder.

7. Click **OK**, then **Apply**.



Note: If a Windows Security pop-up appears, click Yes. The service account will now be able to access this folder.

Note: The application folder only needs Write and Modify permissions during the installation or during an upgrade. You can remove these once the installation process is complete.

Configuring User Rights Assignment

The following settings are required for DelineaPrivilege Manager to function:

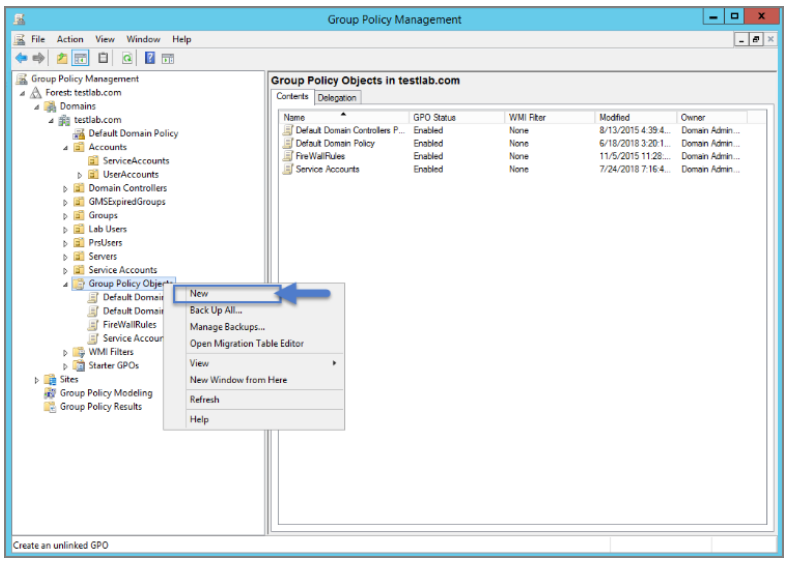
- Log on as a batch job
- Impersonate a client after authentication

You can adjust these settings either

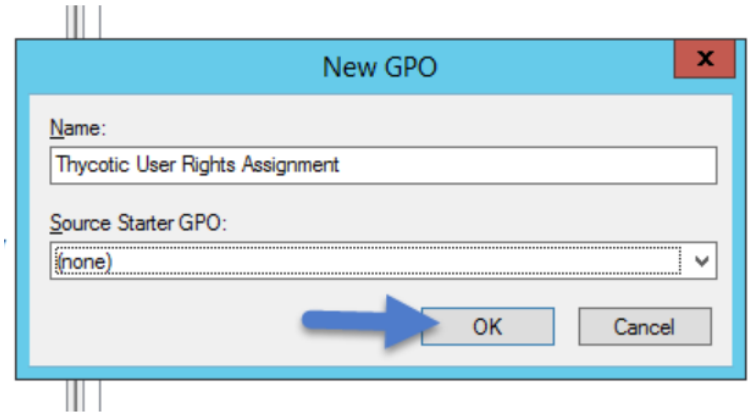
- At the Domain level using Group Policy
- Locally on your IIS Web Server using the Local Security Policy Console

Setting User Rights Assignment on the Domain

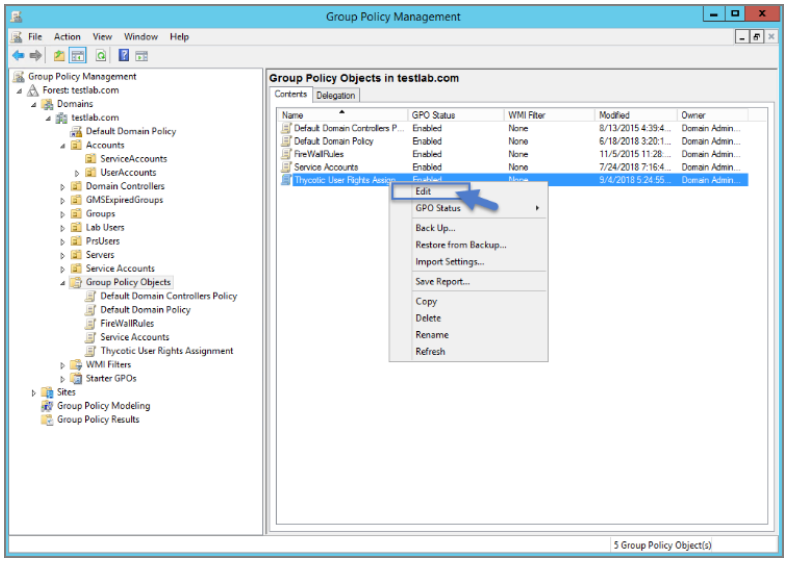
1. Open Group Policy Management Console and right-click your preferred GPO container (i.e. Group Policy Objects).
2. Click **New**.



3. Name the new GPO (i.e., Delinea User Rights Assignment).
4. Click **OK**.
5. Right-click **new GPO**.
6. Click **Edit**.
7. Expand **Computer Configuration** | **Policies** | **Windows Settings** | **Security Settings** | **Local Policies**.
8. Click **User Rights Assignment**.
9. Right-click **Log on as a batch job** and click **Properties**.



10. Ensure that the **Define these policy settings** box is checked
11. Click **Add User or Group**.
12. Add your Delinea Service Account.
13. Click **OK**, then **Apply**.



14. Grant **Impersonate a client after authentication** permission to the service account under "User Rights Assignment" the same way "Log on as a batch job" was assigned above.
15. Link your new GPO to the OU where your Delinea product machine accounts exist (web + database servers).

> **Note:** This will overwrite any configuration in the local security policy. Utilizing the local security policy is a safer option if you are not sure about your usage across your domain.

Setting User Rights Assignment Locally

1. On the web server hosting IIS and your Delinea Application files.
2. Open **Local Security Policy Console** (Run as administrator).

3. Expand **Local Policies** | **User Rights Assignment**.
4. Right-click **Log on as a batch job** | **Properties** | **Add User or Group**.
5. Select your Delinea Service Account and then click **OK**.
6. Do the same to set Impersonate a client after authentication.

   Note: If you get a **Service Unavailable** after applying "Log on as a batch job" permissions, try updating your group policy settings:

   a. Open the Command Console.
   b. Type in **gpupdate /force**.
   c. Restart the Windows Process Activation Service.

Securing the IIS Server

This is a list of items that IIS admin can implement to secure the IIS/Web server.

Patches and Updates

Run Microsoft Baseline Security Analyzer on a regular interval to check for latest operating system and components updates.
The latest updates and patches are applied for Windows, IIS server, and the .NET Framework. (These should be tested on development servers prior to deployment on the production servers.)
Check the Microsoft Security Updates at https://docs.microsoft.com/en-us/security-updates/ on a regular interval for up to date Microsoft technical security notifications.

Services

- Unnecessary Windows services are disabled.
- Services are running with least-privileged accounts.
- FTP, SMTP, and NNTP services are disabled if they are not required.
- Telnet service is disabled.
- ASP .NET state service is disabled and is not used by your applications.

Protocols

- WebDAV is disabled if not used by the application OR it is secured if it is required.
- TCP/IP stack is hardened.
- NetBIOS and SMB are disabled if not used (closes ports 137, 138, 139, and 445).

Accounts

- Unused accounts are removed from the server.
- Windows Guest account is disabled.
- Administrator account is renamed and has a strong password.

- IUSR_MACHINE account is disabled if it is not used by the application.
- If your applications require anonymous access, a custom least-privileged anonymous account is created.
  - The anonymous account does not have write access to Web content directories and cannot execute command-line tools.
- ASP.NET process account is configured for least privilege. (This only applies if you are not using the default ASPNET account, which is a least-privileged account.)
- Strong account and password policies are enforced for the server.
- Remote logons are restricted. (The "Access this computer from the network" user-right is removed from the Everyone group.)
- Null sessions (anonymous logons) are disabled.
- No more than two accounts exist in the Administrators group.

Files and Directories

- Files and directories are contained on NTFS volumes.
- Web site content is located on a non-system NTFS volume.
- Log files are located on a non-system NTFS volume and not on the same volume where the Web site content resides.
- The Everyone group is restricted (no access to `\Windows\system32` or Web directories).
- Web site root directory has deny write ACE for anonymous Internet accounts.
- Content directories have deny write ACE for anonymous Internet accounts.
- Remote IIS administration application is removed.
- Resource kit tools, utilities, and SDKs are removed.

Shares

- All unnecessary shares are removed (including default administration shares).
- Access to required shares is restricted (the Everyone group does not have access).
- Administrative shares (C$ and Admin$) are removed if they are not required.

Ports

- Internet-facing interfaces are restricted to port 80 (and **443** if SSL is used).
- Intranet traffic is encrypted (for example, with SSL) or restricted.

Registry

Remote registry access is restricted.
SAM is secured (`HKLM\System\CurrentControlSet\Control\LSA\NoLMHash`).

Auditing and Logging

- Failed logon attempts are audited.
- IIS log files are relocated and secured.
- Log files are configured with an appropriate size depending on the application security requirement.
- Log files are regularly archived and analyzed.
- Access to the Metabase.bin file is audited.
- IIS is configured for W3C Extended log file format auditing.

Sites and Virtual Directories

- Web sites are located on a non-system partition.
- "Parent paths" setting is disabled.
- Potentially dangerous virtual directories, including IISSamples, IISAdmin,
- IISHelp, and Scripts virtual directories, are removed.
- MSADC virtual directory (RDS) is removed or secured.
- Include directories do not have Read Web permission.
- Virtual directories that allow anonymous access restrict Write and Execute Web permissions for the anonymous account.
- There is script source access only on folders that support content authoring.
- There is write access only on folders that support content authoring and these folder are configured for authentication (and SSL encryption, if required).
- FrontPage Server Extensions (FPSE) are removed if not used. If they are used, they are updated and access to FPSE is restricted.

Script Mappings

- Extensions not used by the application are mapped to 404.dll (.idq, .htw, .ida, .shtml, .shtm, .stm, idc, .htr, .printer).
- Unnecessary ASP.NET file type extensions are mapped to "HttpForbiddenHandler" in Machine.config.

ISAPI Filters

Unnecessary or unused ISAPI filters are removed from the server.

IIS Metabase

- Access to the metabase is restricted by using NTFS permissions `%systemroot%\system32\inetsrv\metabase.bin`).
- IIS banner information is restricted (IP address in content location disabled).

Server Certificates

- Certificate date ranges are valid.
- Certificates are used for their intended purpose (for example, the server certificate is not used for e-mail).
- The certificate's public key is valid, all the way to a trusted root authority.
- The certificate is SHA 256 or better.

Machine.config

- Protected resources are mapped to HttpForbiddenHandler.
- Unused HttpModules are removed.
- Tracing is disabled `<trace enable="false"/>`
- Debug compiles are turned off. `<compilation debug="false" explicit="true" defaultLanguage="vb">`

Code Access Security

- Code access security is enabled on the server.
- All permissions have been removed from the local intranet zone.
- All permissions have been removed from the Internet zone.

Other Check Points

- HTTP requests are filtered.
- Remote administration of the server is secured and configured for encryption, low session time-outs, and account lockouts.

Other Considerations

- Do use a dedicated machine as a Web server.
- Do physically protect the Web server machine in a secure machine room.
- Do configure a separate anonymous user account for each application, if you host multiple Web applications,
- Do not install the IIS server on a domain controller.
- Do not connect an IIS Server to the Internet until it is fully hardened.
- Do not allow anyone to locally log on to the machine except for the administrator.

Actions

In Privilege Manager, taking action is the name of the Application Control game. Once you know how to accurately identify events via filters, the next crucial step in policy creation is to make stuff happen by applying specific actions to your filtered targets. This begs the question: what actions are possible to perform in Privilege Manager?

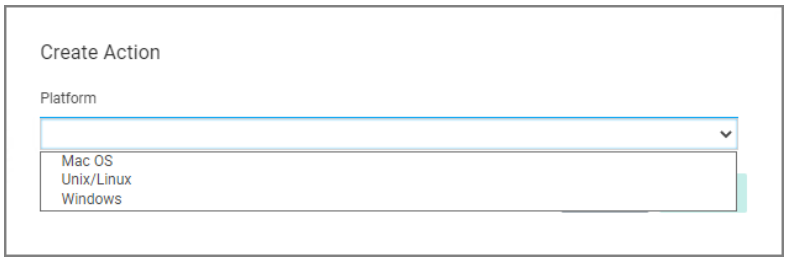
The most popular and well-known action categories in Application Control include:

- **Blocking Actions** - Blocking an application simply means: deny it, or prevent it from running.
- **Monitoring Actions** - This is a category of actions that can be applied to unknown applications that attempt to run. Sandboxing is another term often linked to monitoring, because you can create policies that link to reputation checking tools (like VirusTotal) to perform smart actions once an unknown file's reputation has been verified.
- **Elevation Actions** - Allowing an application to run (allow listing) is good and well for trusted programs, but many trusted applications also require a higher credential set than your end users normally have access to. The elevation action category will allow an application to run with elevated permissions so any user can, for example, install that trusted HP printer on your network without taking time out of a HelpDesk employee's day. Implementing elevation policies allow "Least Privilege" to be implemented by your organization, eliminating the need for local users to have full administrator access on their computer.
- **Workflow Actions** - Some actions explicitly enforce an organization's workflow system. The big example here is the “Request Access” action that will prompt a user for the reason they are trying to access an application for verification purposes and auditing.
- **Display Message Actions** - Display messages are paired with one of the action types listed above. Display Message Actions are customizable and serve to tell the end user what is happening and why.

For a more complete (and more specific) list of all out-of-the-box Privilege Manager actions and types of actions, see the List of Default Actions topic.

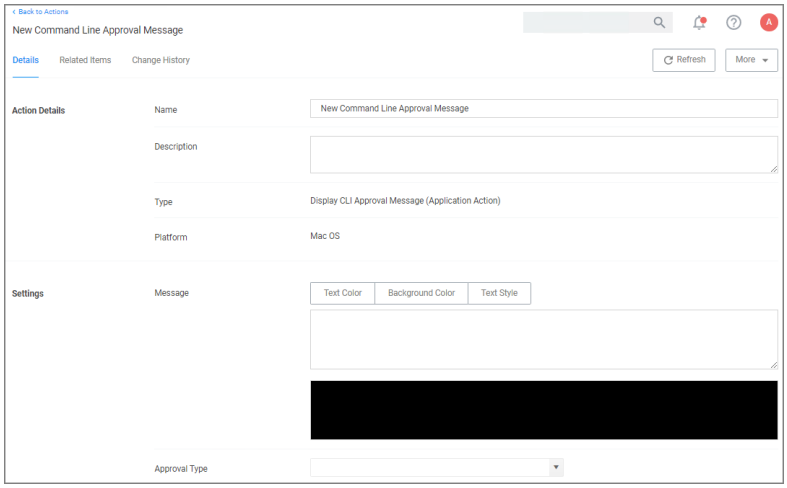
Creating a New Action Manually

1. Navigate to **Admin | Actions** in Privilege Manager and click **Create Action**.
2. From the **Platform** drop-down, select either macOS, Unix/Linux, or Windows.



3. From the **Type** drop-down, select the action type.
4. Name your new action and type a Description, then click **Create**.

Editing options for actions depend on the type of action selected from the drop-down.



Using the Command Line Action Editor

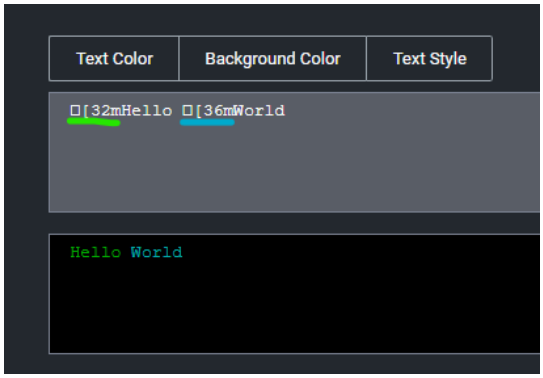
Command Line Action types have a built-in text editor to customize the user experience.

The administrator can customize the:

- Text Color
- Background Color
- Text Style.

By default the background and foreground colors will be based on the user's terminal configuration settings. You can use **Text Style | Reset** to reset to defaults at any point.

The text color can be changed and any color/style customization applies to all text after the specific ANSI control character has been inserted.



Click here for a deep dive on ANSI control codes.

List of Default Actions

This topic describes the out-of-the-box actions that are available in Privilege Manager and can be used to make your policy configuration process easy.

Actions Catalog

Here is the complete list of Actions that come with Privilege Manager out-of-the-box, according to **OS** and category **type**:

macOS

Type	Action	Description
Adjust Effective Process Rights Action	**Run as Root**	Adjust the process rights of the application to run as the root user (macOS)
~~Allow Copy Action~~	**Allow Copy to Applications Directory**	**Note**: This action is deprecated and can only be used with macOS agents versions **prior to 11.2**. This action is used by policies that allow users to copy applications to the root Applications directory as standard users using Privilege Manager.app.
	Allow Package Installation	This action is used by policies that allow users to run the package installer elevated.
Authorization DB Right Action	**Activity Monitor Kill Authorization Right** (com.apple.activitymonitor.kill)	This action grants the com.apple.activitymonitor.kill right in the authorizationdb for the duration of an applicable process.
	Bless Helper Authorization Right (com.apple.ServiceManagement.blesshelper)	This action grants the com.apple.ServiceManagement.blesshelper right in the authorizationdb for the duration of an applicable process.
	Install Apple Software Authorization Right (system.install.apple-software)	This action grants the system.install.apple-software right in the authorizationdb for the duration of an applicable process.
	Modify System Keychain Authorization Right (system.keychain.modify)	This action grants the system.keychain.modify right in the authorizationdb for the duration of an applicable process.

Type	Action	Description
	Xcode FLE Authorization Right (com.apple.dt.Xcode.LicenseAgreementXPCServiceRights)	This action grants the com.apple.dt.Xcode.LicenseAgreementXPCServiceRights right in the authorizationdb for the duration of an applicable process.
CLI Justification Message (Application Action)	**Command Line Justification Message**	Justification message to execute before allowing the process to continue.
Display Advanced Message Action	**Application Approval Request (with Offline Fallback) Message Action**	Application Approval Request Message Action for macOS.
	Application Approval Request (with ServiceNow Request Item Number) Message Action	This action will display an approval request form for ServiceNow integrations for approval before allowing application to run on macOS endpoints.
	Application Approval Request Message Action	Application Approval Request Message Action for macOS.
	Application Denied Message Action	This action will display a modal denial notification message to the user and prevent application execution on macOS.
	Application Justification Message Action	Application Justification Message Action for macOS.
	Application Warning Message Action	Application Warning Message Action for macOS.
Just in Time Group Membership Action	**Just in Time Group Membership Action**	This action will add a user to a specified group for a specified time.
Display User Message Action	**Deny Execute Message**	This action displays a message to the user informing them that an application has been denied execution

Type	Action	Description
Deny Execute Action	**Deny Execute**	This action stops specified applications from executing
Quarantine File Action	**File Quarantine**	This action can be used to quarantine a file by moving it to the default agent quarantine path

Windows

Type	Action	Description
Adjust Process Rights Action	**Add Administrative Rights**	This action adds basic administrative rights needed to install and run specified applications
	Add Administrator Rights - Unrestricted	This action adds administrative rights at a higher integrity level for specified applications. Usually you will only need to use this type of action if an application or installer needs to create a global object, such as a service, or if system changes require unrestricted administrator rights
	Remove Administrator Rights	This action removes administrative rights for specified applications
	Remove Advanced Privileges Action	This action removes advanced privileges for specified applications from the process token
Application Verifier Action	**Application Compatibility Testing**	This action triggers application compatibility testing while the process runs and sends the results to the server
Apply SVS Layer Action	**Workspace Virtualization Global Layer**	This action places specified applications in a common Workspace Virtualization global layer
	Workspace Virtualization Isolation Layer	This action places specified applications in a common Workspace Virtualization isolation layer

Type	Action	Description
Create Children Processes as User	**De-elevate Child Processes**	Ensures that all child processes are created without administrator rights. Forces all new processes created by the targeted application to be launched by a de-elevated token.
Deny Execute Action	**Deny Execute**	This action stops specified applications from executing
Deny File Access Action	**Deny Read/Write Access to Microsoft Office Document Files**	This action can be used to deny read and write access to Microsoft Office documents
	Deny Write Access to Executable Files	This action can be used to deny write access to common executable files
Deny Windows Hooking Action	**Deny Windows Hooking**	This action limits specified applications from interacting in malicious ways with other applications
Display Advanced (Xaml) Windows Message	**Application Denied Message Action**	This action will display a modal denial notification message to the user and prevent application execution on Windows
	Application Denied Notification Action	This action will display a notification to the user that the process has been denied by a policy. The notification window will fade in and out and automatically close after a period of time
	Application Warning Message Action	Application Warning Message Action for Windows.
	Approval Request (with Offline Fallback) Form Action	This action will display an approval request form for approval before allowing application to run.
	Approval Request (with ServiceNow Request Item Number) Form Action	This action will display an approval request form for ServiceNow integrations for approval before allowing application to run.

Type	Action	Description
	Approval Request Form Action	This action will display an approval request form for approval before allowing application to run
	Authenticated Justification Message Action	This action will display a customized message to the user, allowing for feedback and requiring authentication before running an application
	Group Member Authenticated Message Action	This action will display a customized message to the user and requires authentication by a member of the specified group if the end-user is not a member
	Justify Application Elevation Action	This action will display a justification prompt to the user before continuing to the process controlled by a policy
	Justify Application Message Action	This action will display a justification prompt to the user before continuing to the process controlled by a policy
	Mobile Approval Request Form Action	This action will display a approval request form for approval before allowing application to run.
Display User Message Action	**Deny Execute Message**	This action displays a message to the user informing them that an application has been denied execution
	Deny Files Read and Write Access Message	This action displays a message to the user informing them that an application will be restricted from certain file access
	Limit Process Rights for New Applications Message	This action displays a message to the user informing them that an application has had its rights reduced
	Quarantine Message	This action displays a message to the user informing them that an application has been quarantined
	Remove Rights Message	This action displays a message to the user informing them of an associated action

Type	Action	Description
	SWV Global Layer User Message	This action displays a message to the user informing them that an application has been placed in SWV global layer
	SWV Isolation Layer User Message	This action displays a message to the user informing them that an application has been placed in SWV isolation layer
	Windows Hooking Message	This action displays a message to the user informing them that an application will be stopped from interacting with other applications
Encrypt Application Files	**Encrypt Common Application Documents**	This action can be used to automatically encrypt common application documents using Windows EFS.
	Encrypt Microsoft Office Documents	This action can be used to automatically encrypt Microsoft Office documents using Windows EFS.
Execute Application Action	**Immediate File Inventory**	This action will inventory the file being executed
GenericDetourAction	**Enable UAC Virtualization**	This action will turn on UAC virtualization for the target process.
Meter Application Action	**Meter Application Usage**	This action meters the usage of the specified applications
Quarantine File Action	**File Quarantine**	This action can be used to quarantine a file by moving it to the default agent quarantine path
Restrict File Dialogs	**Restrict File Dialogs**	This action prevents users from abusing the elevated rights of the application via the file open and save dialogs. This is a recommended action that customers should add to their elevation policies.
Set Environment Variable Action	**Suppress User Account Control Consent Dialog**	This action will prevent the UAC consent dialog from being displayed.

Type	Action	Description
Set Process Security Descriptor Action	**Locked down Service Process Security Descriptor**	This action applies a restrictive security descriptor disallowing Administrators the right to terminate the process.
Win32 API Control Action Examples	**Block Local User Management**	This is a new action that, when applied, blocks the target process from adding, removing, or modifying local users. The powershell "'*localuser*'" cmdlets are what this action will block. It will block these actions from any application including Windows utilities, command-line utilities, etc.
	Block Local Group Management	This is a new action that when applied block the target process from adding, removing, modifying, or changing the membership of local groups. The powershell "'*localgroup*'" cmdlets are what this action will block. It will block these actions from any application including Windows utilities, command-line utilities, etc.
	Block LSA Privilege Management	This is a new action that when applied blocks the target process from changing local privileges. It will block these actions from any application including Windows utilities, command-line utilities, etc.

Unix/Linux

Type	Action	Description
Display User Message Action	**Deny Execute Message**	This action displays a message to the user informing them that an application has been denied execution
Deny Execute Action	**Deny Execute**	This action stops specified applications from executing

Action Message Localization

Action messages can be localized for user interaction on endpoints. For this to work, create a duplicate the **Approval Request Form Action** and then view and modify the XML of that duplicated item.

If you look at the xml example code below, you will the `<axc:LocaleResourceCollection x:Key="LocaleResources">` element with one child `<axc:LocaleResourceSet>`. This child is the default language for the approval request, which is English.

To add a localization such as Spanish:

1. Copy the `<axc:LocaleResourceSet>` element block including the `</ axc:LocaleResourceSet>` element.
2. Paste it underneath `</ axc:LocaleResourceSet>`.

3. Add `Language="es"`, as in `<axc:LocaleResourceSet Language="es">`.
4. Modify the elements with string values to the correct translation for that language.

For a list of valid language code values, refer to https://docs.microsoft.com/en-us/openspecs/office_standards/ms-oe376/6c085406-a698-4e12-9d4d-c3b0ee3dbc4a (the more specific language is used first, such as 'es-ES' for Spanish - Spain and then the broader 'es' will be used if a specific language translation is not found, the last resort is the invariant translation).

Example for Spanish


```
<CustomXamlExecutionActionContract xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schema
instance" xmlns="http://schemas.arellia.com/dc/ApplicationControl/ApplicationAction/">
<adc:Attributes>NoReplication System</adc:Attributes>
<adc:Description>This action will display a approval request form for approval before allowing applica
<adc:FolderId>cf02777a-86b3-4450-b5af-1dcbee252071</adc:FolderId>
<adc:ItemId>5d4e0cb0-604b-4fc4-968c-e68a8b5c7838</adc:ItemId>
<adc:Name>Approval Request Form Action (with Localization)</adc:Name>
<adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
<adc:Strings/>
<adc:Tags/>
<AdjustSession>false</AdjustSession>
<Commandline>/approvalTypeId:2A3F33C4-15DD-41D0-A620-889EA1E4408A</Commandline>
<Executable>.\ArelliaDisplayXamlAction.exe</Executable>
<TerminateExitCode>1</TerminateExitCode>
<WaitOnApplication>true</WaitOnApplication>
<ChildAssociations/>
<OfflineApprovalType>OfflineNotAllowed</OfflineApprovalType>
<OwnsItemIds/>
<RequireLogon>false</RequireLogon>
<UserGroupId i:nil="true"/>
<Xaml>
```

```
<![CDATA[ <Window xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation" xmlns:x="http://s
compatibility/2006" mc:Ignorable="ac acs" Icon="Images/thycotic-icon.png" WindowStartupLocation="Cent
<axc:StringKeyedResource Key="ReasonLabel" Value="Reason (required):" /> <axc:StringKeyedResource Key=
Key="InstructionTextSection"> <axc:StringKeyedResource.Value> <Section xml:space="preserve"> <Paragra
Key="CancelButtonLabel" Value="Cancel" /> <axc:StringKeyedResource Key="RefreshButtonLabel" Value="Re
xml:space="preserve"> <Paragraph><Run>A previous request for this application has been submitted for
<axc:StringKeyedResource Key="ReasonLabel" Value="Motivo (requerido):" /> <axc:StringKeyedResource Ke
<axc:StringKeyedResource.Value> <Section xml:space="preserve"> <Paragraph><Run>Escriba una breve expl
Value="Cancelar" /> <axc:StringKeyedResource Key="RefreshButtonLabel" Value="Recargar" /> <axc:String
<Paragraph><Run>Se ha enviado una solicitud previa para esta solicitud para su revisión.</Run></Parag
Value="25" /> <Setter Property="MinWidth" Value="85" /> </Style> <Style x:Key="ReadOnlyFieldStyle" Ta
Property="IsReadOnly" Value="True" /> <Setter Property="IsTabStop" Value="False" /> </Style> <!-- spe
x:Key="EncodedLogoImage">iVBORw0KGgoAAAANSUhEUgAAAQcAAABYCAIAAAB3ZqVmAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
E+KKFgRbnwEinf8kMjc3B92Nj7iiQ8HWZ4CoU0nrCtd1scFMfPnll9CZsHVF5Mqg+tiMq+wZLkHGUd8b/vZw2iZdssyw5pFFsPUZI
uoKAqlDIMBQlCvUcSvNZCYN27dvV2nDhLd8AuF14NaH6imhWuewK6zWP1gpH3zmga4GNeTjjz9GLDdIOi+wrqBNSb25zvT0NNaOAb
27UMsAUQyETbTrWHHx4kXUMkCnI664BnQxEDYBRQgEGApxRTOO5e3qClTxQKdDruBmmzKDAgibgCIEAgwyVkRAjAEiHcR4lCzNeTO
SQYwHugBU8UDXkogr7NqFWgaIcoBEDBDFQJgBIh3EGCDSQYwHugBU8UDXkogr7NqFWgaIcpDwzDkBUQyEGSDSQYwBIh3EeKALQBUP
ICgbAXWQ/KOPPkLMxNDQEKQ6CDNApIMYD3Q1UMsAkQ5iDBDFcMslOu2mNxNv0ml0tPdzRS1rpINcgXeWIHsIBEzQt3z++efhXmvlu
u/Zs+fcuXNYLAQ55+DBg5VKJay3hZattyghT56vUFCGDEkaLlLf7PS6evXqY8eOXb16lTZO3Sfqzbvvvrtlyx YlJupvTJQct5zZEl
lxRcDevXvrTqhflUKMoa7vHIKjqveLlT+p9/gOhSY29Dp1ulsdlYuF+nGGW9e7TvXQicTS6A7O/JGw5E7MdoYrCPTlgnjvvfeQt/N
zlbRl8tRXqtWlyMLjlPtd/z8JSlajROC94Fd4p4vsyeIKIRX+n2i4pfGZnomT3RMn6dWuVJYtQSIGmjg5jkud2+r/zsgSk8EoUext
Hh7vF1cI+XArnutsfuXWLQdvo9dO5fbarcBov08udIZdHSj+9xtxxBVCAdCI8ccDd9TK7VzZ9LfbHn359izn1sE97BUP/Bjf12TEF
K5CYII=</sys:String> <!-- heading --> <Style x:Key="MainWindowPanelStyle" TargetType="Panel"> <Setter
Value="8" /> <Setter Property="Background" Value="Yellow" /> </Style> <Style x:Key="TitleHeadingStyle
Property="Padding" Value="8" /> <Setter Property="Background" Value="#3d3d3d" /> </Style> <Style x:Key
x:Key="InformationRichTextBoxStyle" TargetType="RichTextBox" BasedOn="{StaticResource BaseRichTextBox
{StaticResource LocaleResources}}" /> </Style> <Style x:Key="ApplicationFieldStyle" TargetType="TextB
[UserLabel],Source={StaticResource LocaleResources}}" /> </Style> <Style x:Key="UserNameFieldStyle" T
BaseRichTextBoxStyle}"> <Setter Property="Margin" Value="0,8,0,0" /> </Style> <Style x:Key="ReasonLab
Property="AcceptsReturn" Value="True" /> <Setter Property="Height" Value="64" /> <Setter Property="Sc
ReasonText,Mode=TwoWay,UpdateSourceTrigger=PropertyChanged}" /> </Style> <Style x:Key="GeneralErrorIn
TargetType="Grid"> <Setter Property="Visibility" Value="Collapsed" /> </Style> <SolidColorBrush x:Key
DefaultBackgroundBrush}" /> <Style x:Key="ApprovalStatusBorderStyle" TargetType="Border"> <Setter Pro
x:Key="ApprovalStatusLabelStyle" TargetType="TextBlock"> <Setter Property="Text" Value="{Binding [App
Value="White" /> <Setter Property="Text" Value="{Binding ApprovalStatus}" /> <Setter Property="Vertic
x:Key="ContinueWithReasonButtonStyle" TargetType="Button" BasedOn="{StaticResource BaseButtonStyle}">
BaseButtonStyle}"> <Setter Property="Content" Value="{Binding [ContinueButtonLabel],Source={StaticRes
LocaleResources}}" /> <Setter Property="Command" Value="{Binding RefreshApprovalCommand}" /> <Setter
<Window.FlowDirection> <Binding Path="[FlowDirection]" Source="{StaticResource LocaleResources}" /> <
<ColumnDefinition Width="Auto" /> </Grid.ColumnDefinitions> <Border Style="{StaticResource TitleHeadi
{StaticResource ContentPanelStyle}"> <!-- Information of why this dialog needs attention --> <RichTex
<ColumnDefinition Width="Auto" /> <ColumnDefinition Width="*" /> </Grid.ColumnDefinitions> <Grid.RowD
ac:VisibilityHelper.HiddenWhenTrue="{Binding IsPendingApproval}" adx:VisibilityHelper.HiddenWhenTrue="
{StaticResource ReasonLabelStyle}" /> <TextBox Style="{StaticResource ReasonTextBoxStyle}" adx:FocusH
<RichTextBox Style="{StaticResource ApprovalRequestStatusInformationRichTextBoxStyle}" ac:RichTextBox
<Grid.ColumnDefinitions> <ColumnDefinition Width="Auto" /> <ColumnDefinition Width="*" /> </Grid.Colu
BottomActionPanelStyle}"> <Grid.ColumnDefinitions> <ColumnDefinition Width="Auto" /> <ColumnDefinitio
IsPendingApproval}" adx:VisibilityHelper.HiddenWhenTrue="{Binding IsPendingApproval}" adx:ButtonHelpe
</Xaml>
</CustomXamlExecutionActionContract>
```


Open this link to access, copy, or download the example xml.

Microsoft Entra ID Authentication

This action enables single or muli-factor authentication for Windows and macOS, using Microsoft Entra ID. You are able to customize the message presented to the user when authentication is requested.

The configuration of Entra ID authentication requires the following steps:

- "Step 1 - Registering Your Application with Entra ID" below
- "Step 2 - Creating the Authentication Action" on the next page
- "Step 3 - Configuring Application Policies for Authentication" on page 510

Prerequisites

- You will need access to your organization's Entra ID tenant. Refer to the Microsoft documentation if required.
- You will need to register a new application for your Entra tenant that will be used in this integration. See "Step 1 - Registering Your Application with Entra ID" below.
- Privilege Manager and Privilege Manager agent version 12.0 is required.

Step 1 - Registering Your Application with Entra ID

The Microsoft identity platform performs identity and access management (IAM) only for registered applications. Registering your new custom application establishes a trust relationship between your application and the Microsoft identity platform, with Entra.

Refer to Register an application in Microsoft Entra ID for complete instructions for registering your custom application.

Entering Parameters from the Application Home page.

Parameters specific to Privilege Manager, should be set in the Entra admin center. These parameters are found on the following pages, accessed from the left panel of your application's Home page.

Application page | Register an application

- For **Supported account types,** select **Accounts in this organizational directory only (<your tenant name>)**. Delinea recommends using a single tenant, where only users from this tenant are allowed to use the application.

Overview page

Make a note of the following values.

- **Application (client) ID** (you can use copy to clipboard)
- Select the **Endpoints** tab and in the Endpoints panel, note the **OpenID Connect metadata document URL**.

These two parameters will be requested by Privilege Manager when configuring the Entra action.

Authentication page

- Disable **Allow public client flows** (set to **No**).
- **Add a platform** and specify **Mobile and desktop applications**. Enable **nativeclient** and **MSAL only**.
- **Add a platform** and specify **Single-page application**. For this platform, configure any **Redirect URIs** for the application (for example, `https://localhost/`). This is not a functional URI in the application. This allows Entra to display this application on the Conditional access page.

- **Add a platform** and select **iOS / macOS**. For this platform, enter `com.thycotic.privilegemanagergui` in the **Bundle ID** field,

Expose an API page

- Select **Expose an API**. Click **Add** next to the **Application ID URI** field. In the Edit application ID URI panel, click **Save** to accept the default URI used to identify your web API.
- **Add a scope** and supply `privman.action.auth` for **Scope name**. This is the permission that the Privilege Manager agent application uses during the authentication process, associating the Entra ID with the application resource. This helps the application of the Entra ID Conditional Access policies when targeting an application. Refer to "Conditional access page | Overview" below.
- Supply an **Admin content display name** and **Admin consent description** for use in Microsoft Entra admin center.

API permissions page

- **Add a permission**. Select the application you created (**APIs my organization uses** tab).
- Enable the check box for **privman.action.auth**.
- **Grant admin consent** for your application.

Conditional access page | Overview

A Conditional Access policy targets the application so that Entra requests a second factor of authentication (MFA) before a user is granted access to an application. Refer to Create a Conditional Access Policy for complete instructions.

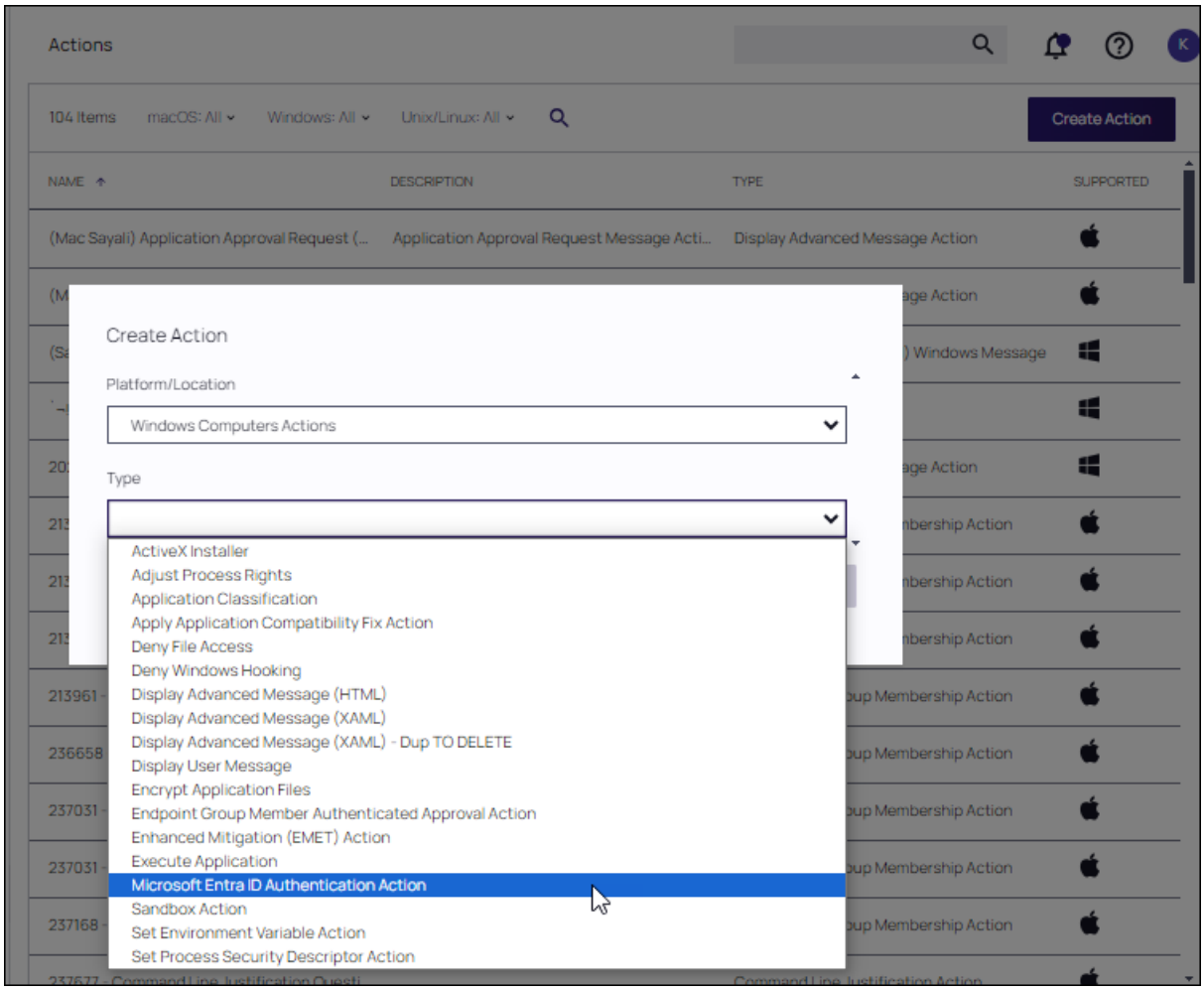
Note: Session controls are not supported by Privilege Manager.

- Enable **Grant access**.

  Select **Policies**, then **Create new policy**.
- Configure the following for the new policy: **Name**, **Users** (specify users and groups), **Target resources** (specify the application), and **Grants** (specify multi-factor authentication).
- Set **Enable policy** to **On.**

Step 2 - Creating the Authentication Action

In Privilege Manager, create an custom Entra ID Authentication action for your application. Navigate to **Admin** | **Actions** and click **Create Action**. Select your platform at the **Create Action** drop-down.



Next, select **Microsoft Entra ID Authentication Action** at the **Create Action** pull-down.

The **Create Action** dialog presents the following required parameters.

- **Entra ID Application/Client ID**
  This is the **Application ID URI** from Entra.
- **Entra ID Authority URL**
  This is the **OpenID Connect metadata document URL** from Entra.

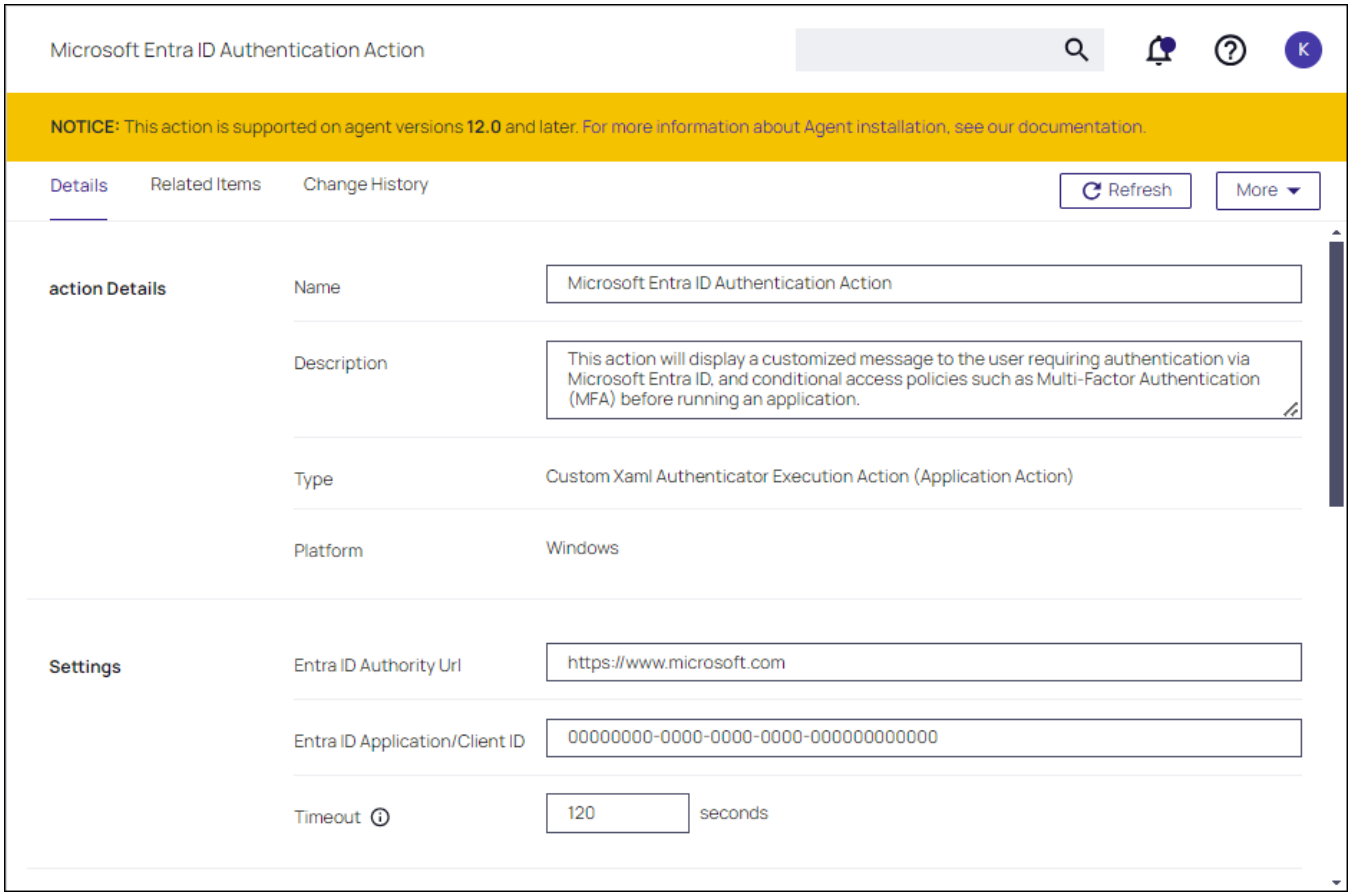
> These are the values you copied from the Application Overview page when registering your application. See "Overview page" on page 507.

Enter these values then click **Create**.

After the action is created, your custom Microsoft Entra ID Authentication action page is displayed. Any of the Entra ID authentication settings can be edited and customized, as well as the authentication messaging.

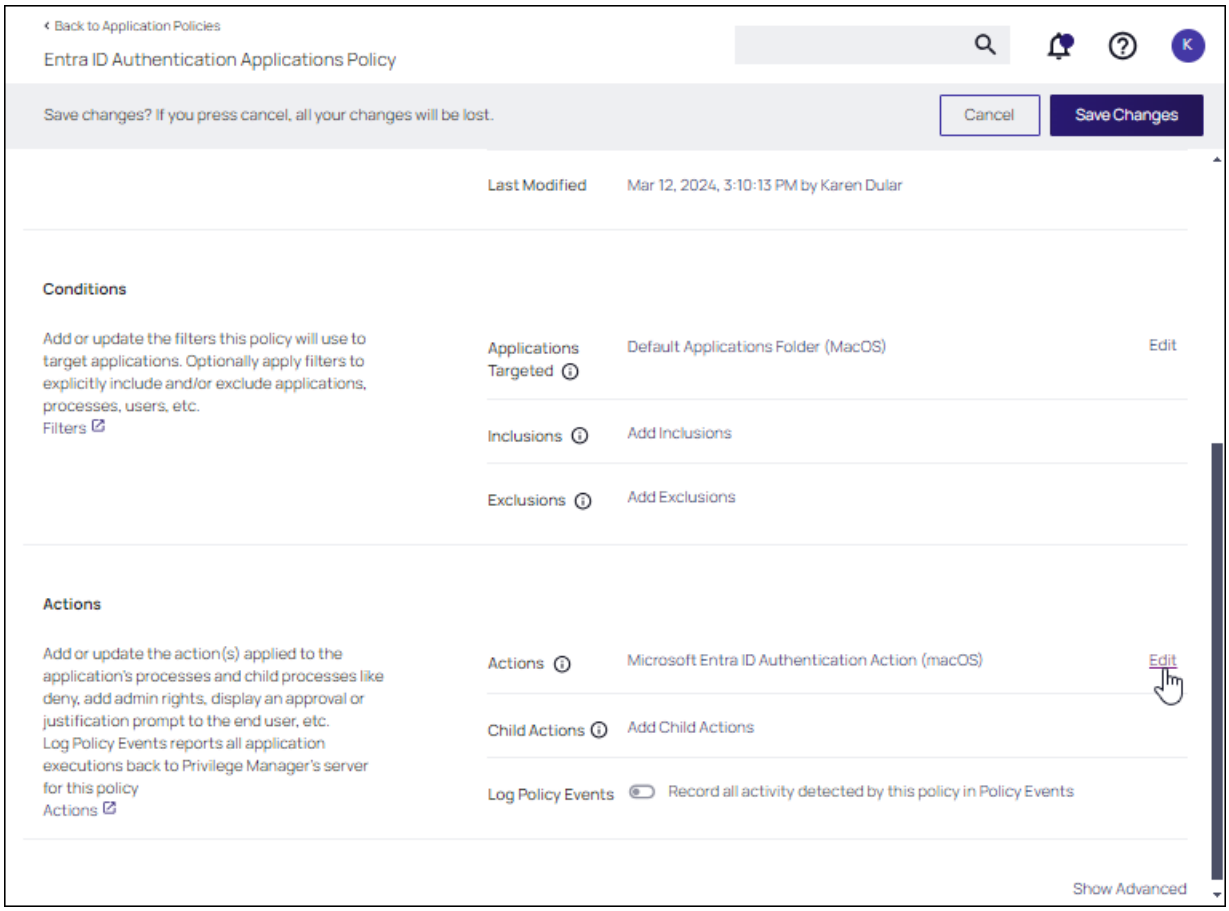
- **TImeout** - After the user clicks **Authenticate**, this is the time the user has to finish authenticating before the authentication is canceled, and the application is blocked from opening.
- For macOS applications, you are able to customize the message, as with other advanced message actions..

Click **Save Changes**, if updates were made.



Step 3 - Configuring Application Policies for Authentication

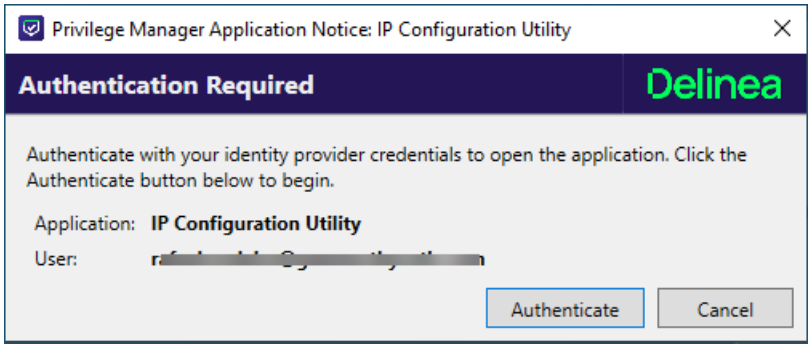
Identify the Application Policy that requires Entra ID authentication. In the **Actions** section of the policy, ensure the **Actions** field is configured for the Entra ID action you created. **Edit** if necessary.



Initiating an Entra ID Authentication

Whenever a policy with an application that requires authentication with an Entra ID is initiated, the following message is presented to the user. Click **Authenticate**.

Supply the requested credentials for authentication.



Message Actions

Messages are common application actions used in Privilege Manager. These messages are presented for end users on their endpoints. There are two kinds of messages:

- Basic, these display as smaller pop-ups directly form the taskbar area. They display and fade automatically. From the Action Type drop-down these are the Display User Message actions for both Windows and macOS.
- Advanced, these messages display as a user dialog, requiring users to justify access to a certain application or to warn the user. Most of these messages require user interaction, but some can be set to fade in and out for the end user. From the Action Type drop down these are the Display Advanced Message for Windows and Display Advanced User Message (macOS) for macOS endpoints.

Note: To use the Windows based WYSIWYG advanced message actions that utilize the rich-text editor, the 11.2 based Application Control Agent needs to be installed.

Rich text or HTML based message editing is detailed for the specific message types under these topics:

- WYSIWYG macOS Action Message Editor
- WYSIWYG Display Advanced Message Action Editor

Both basic and advanced messages are useful for providing feedback to users that an application is being blocked, usage of the application is being logged, or any message that the end user should see.

Basic vs. Advanced Messages

Basic messages briefly pop up from the end user's task bar. They display like other Windows notifications, are shown on the screen, and then disappear without any user interaction required.

Basic messages do not include custom branding or logos. It is easiest to edit basic messages via Privilege Manager's UI. However, the default message may suffice for some use. Basic messages only display a message. These messages do not perform an action. For example, the basic Deny Execute Message should be used in conjunction with the Deny Execute action.

Advanced messages display as a new dialog, typically in the center of the screen, and usually require an interactive action from the end user – entering a justification, enter credentials, waiting for approval, selecting a continue or cancel button, etc.

Advanced message actions are used for justification and approval policies. The ‘Application Denied Notification Action' is the only default advanced message that does not require an interactive action from the end user. While this message has a cancel button to remove the message, this message will fade from the user's screen after a short period of time.

Advanced messages include branding, which can be customized. Some fields are recommended to edit in the XML instead of the UI. These details are expanded in the section on Customizing Advanced Messages.

Types of Advanced Message Actions

There are three categories of advanced messages:

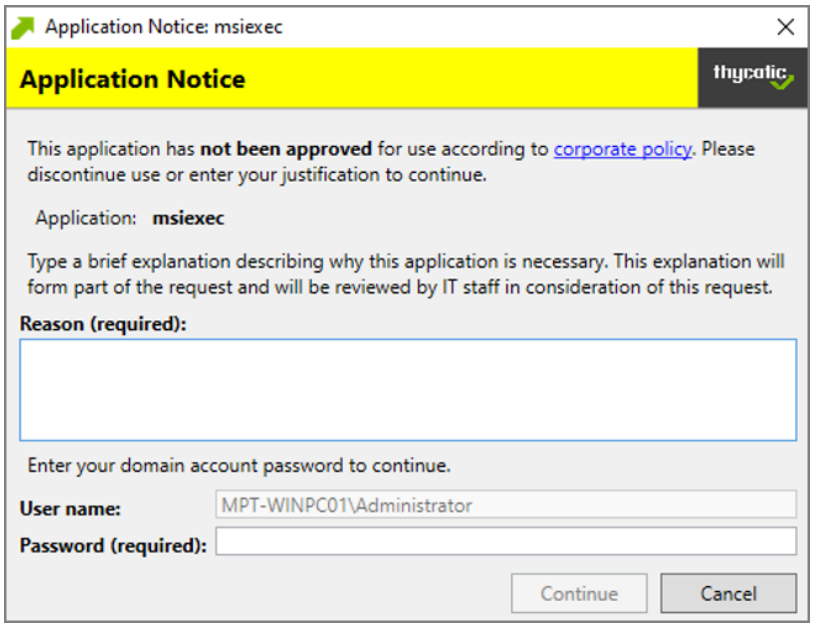
- Advanced Feedback Messages – require information from the end user.
- Approval Request Messages – require information from the end user and approval from the application support team.
- No Required Input Messages – display information to the end user, but do not require information from the end user. May require a button push to clear the message.

Advanced Feedback Messages

Advanced feedback messages require users to justify their need to use an application.

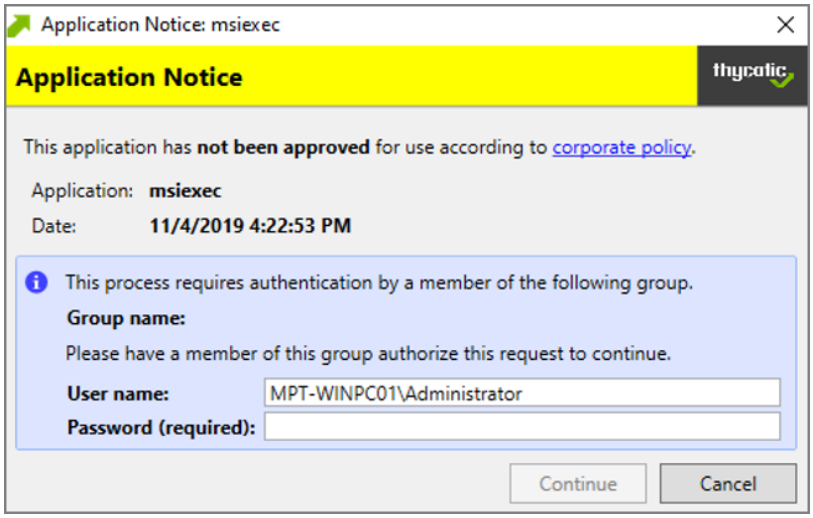
Authentication Justification Message Action

This action will display a customized message to the user, allowing for feedback and requiring authentication before running an application.



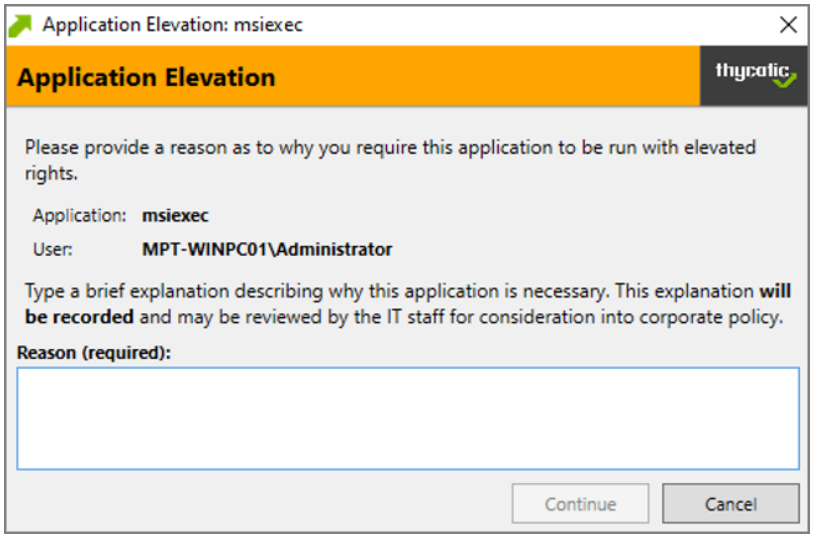
Group Member Authenticated Message Action

This action will display a customized message to the user and requires authentication by a member of the specified group if the end-user is not a member. This process is also known as an over-the-shoulder request, meaning that the end-user will have to get their boss or a member of a specific domain user group to approve the request.



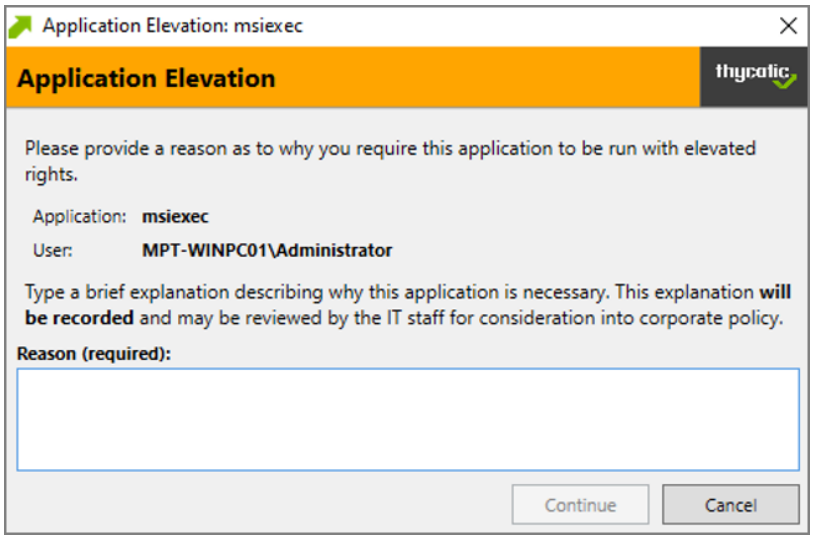
Justify Application Elevation Action

This action will display a justification prompt to the user before allowing the application to run. The Justify Application Elevation Action is to be used with the User Requested Run As Administrator filter in an application control policy. This action collects information from users and creates reports on the server for approval requests.



Justify Application Message Action

This action will display a justification prompt to the user before allowing the application to run. It is used to collect information from users and create reports on the server with reasons why a user was running an application that hasn't been approved or denied yet.



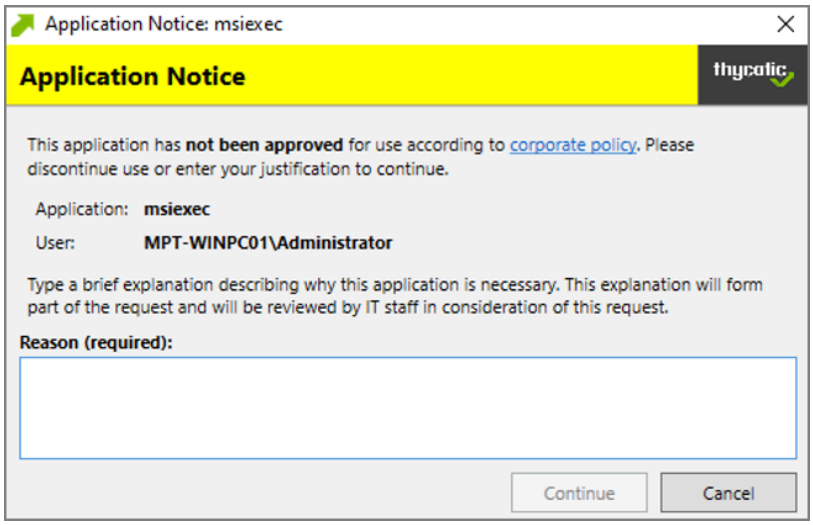
Approval Request Messages

The approval request messages are similar to the justification messages because they both gather feedback from end users and report it in the Privilege Manager console. Approval request messages also allow for end-users to

see a waiting screen until their request has been either approved or denied.

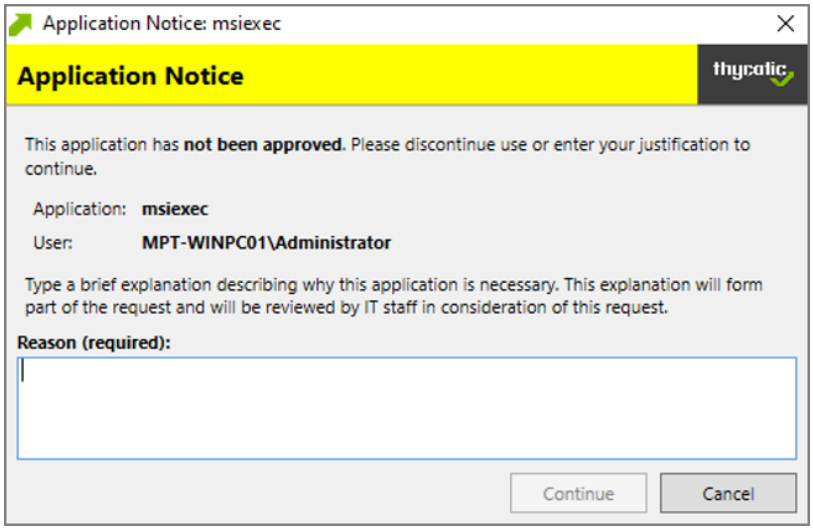
Approval Request Form Action

This action will display a customized message to the user, allowing for feedback and requiring authentication before running an application.

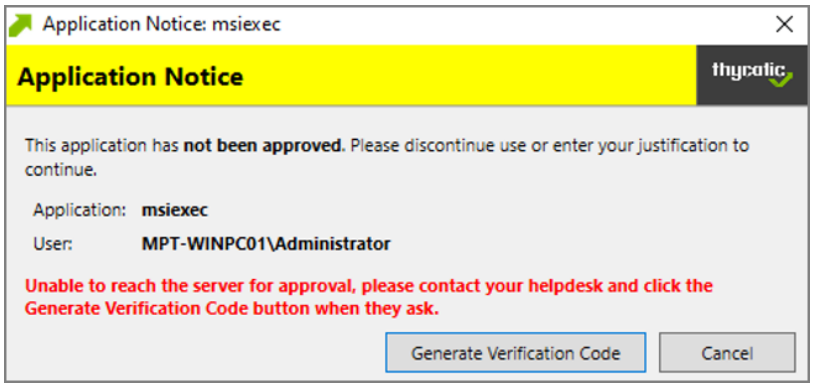


Approval Request (with Offline Fallback) Form Action

This action displays an approval request form before allowing the application to run. These messages will then show a waiting screen until the request is either approved or denied by the appropriate Privilege Manager user/admin. With this advanced message, the same dialogue box as the Approval Request Form Action will appear:



If the machine is offline or can't connect to Privilege Manager to upload the request, another dialogue box will then appear to prompt the end user to contact the helpdesk and generate a verification code:

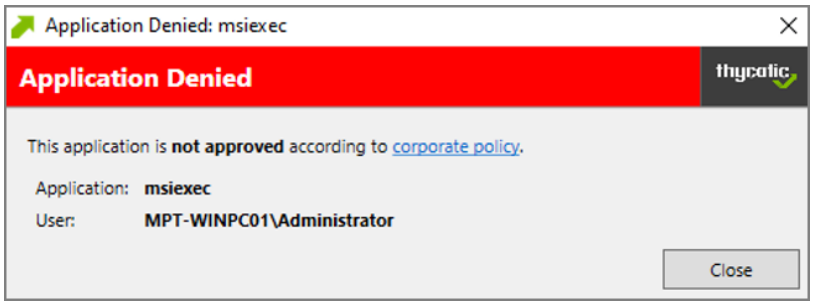


No Required Input Messages

No required input messages differ from the advanced feedback message actions because they do not require a justification to continue. End users need only acknowledge the displayed message. This feature requires that the Microsoft .Net Framework is installed on client machines.

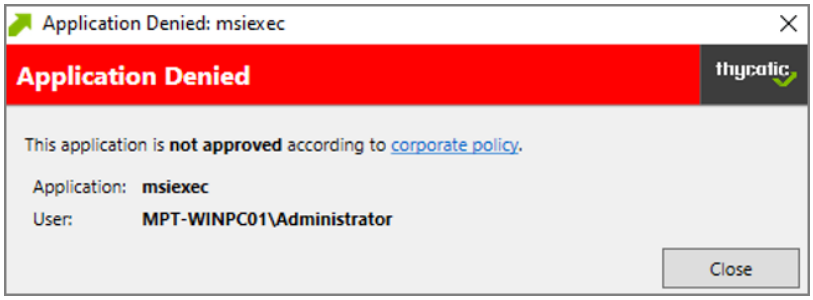
Application Denied Message Action

This action stops an application from being launched and will display a notification of denial to the user attempting to run a process controlled by a policy.



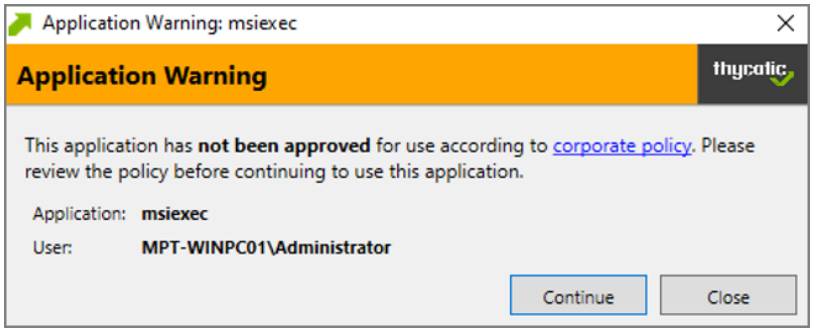
Application Denied Notification Action

This action will display a notification to the user that the process has been denied by a policy. The notification window fades in and out automatically and will close after a defined period of time.



Application Warning Message Action

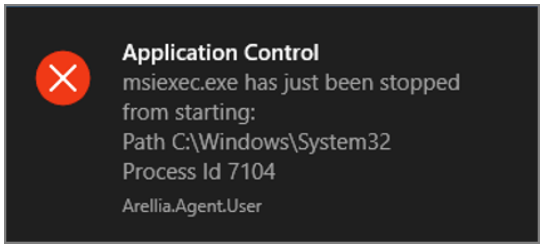
This action will display a warning to the user before allowing the application to run.



Types of Basic Messages

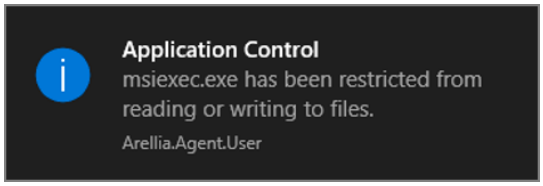
Deny Execute Message

This action displays a message to the user informing that an application has been denied execution. The Deny Execute Action needs to be used with this message.



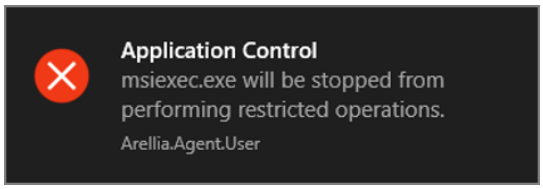
Deny Files Read and Write Access Message

This action displays a message to the user informing that an application will be restricted from certain file access. The Deny Read/Write Access to Microsoft Office Document Files Action needs to be used with this message.



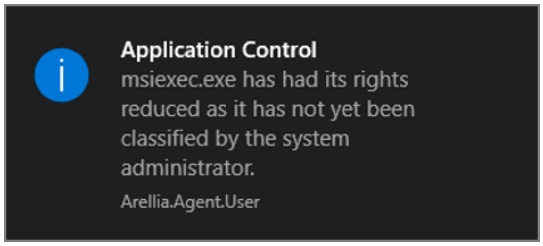
Windows Hooking Message

The action displays a message to the user informing them that an application will be stopped from interacting with other applications. The Deny Windows Hooking Action should be used with this message.



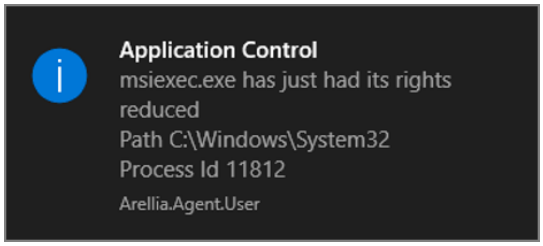
Limit Process Rights for New Applications Message

This action displays a message to the user informing that an application has had its rights reduced. The Remove Administrator Rights or Remove Advanced Privileges Action needs to be used with this message.



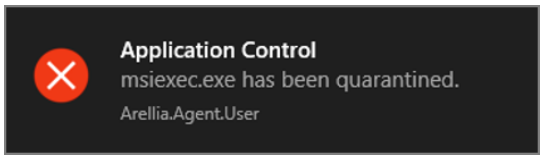
Remove Rights Message

This action displays a message to the user informing them of an associated action. The Remove Administrative Rights Action or Remove Advanced Privileges Action should be used with this message.



Quarantine Message

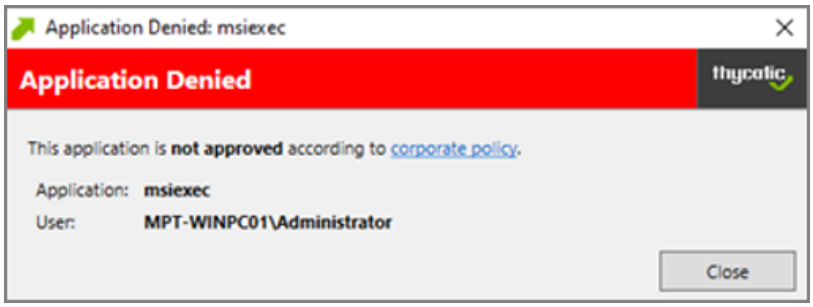
This action displays a message to the user informing that an application has been quarantined. The File Quarantine Action should be used with this message.



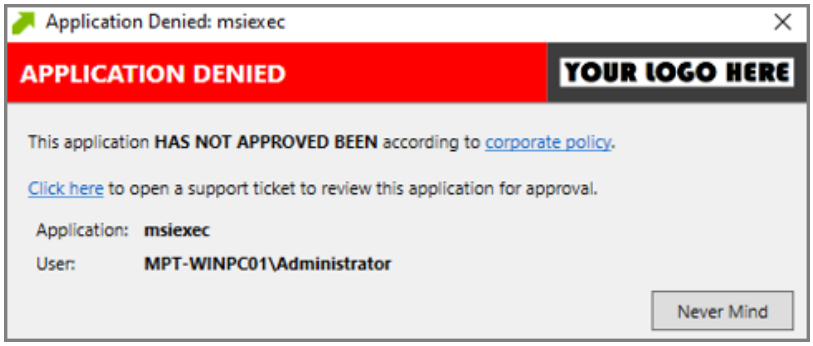
Create Custom Notifications

The default Application Denied Notification Action can be edited/replaced by a customized notification action to better suite a specific customer need.

Example of Default Notification:



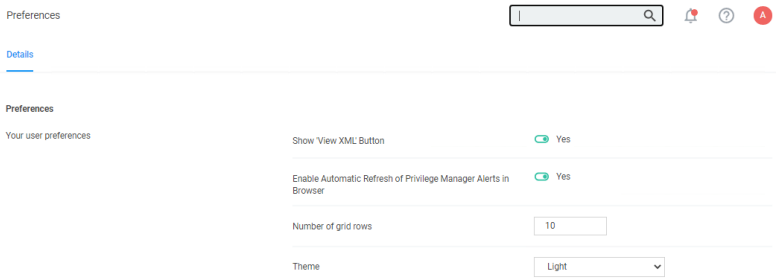
Example of Custom Notification:



Enable View as XML

To edit the message text the **View as XML** button has to be enabled in your console.

1. Navigate to and click your user icon, select **Preferences**.
2. Verify **Show 'View XML' Button** is set to **Yes**, if set to No change the switch.

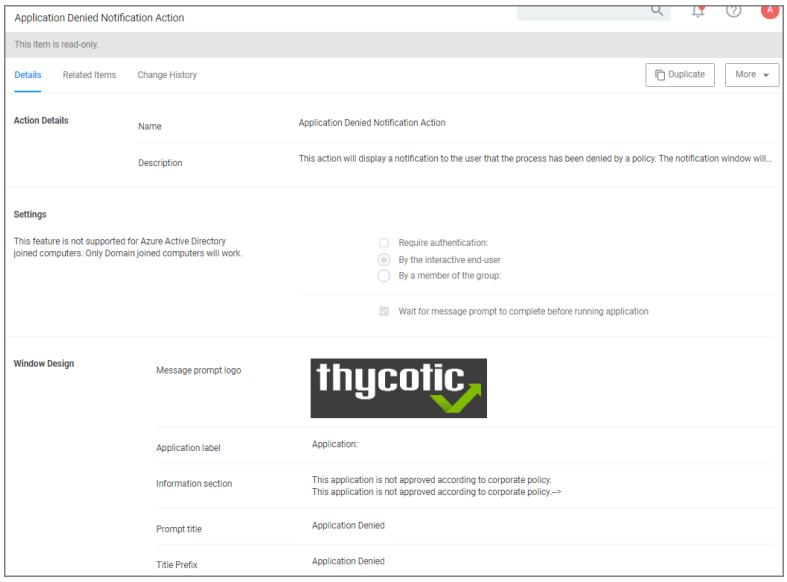


3. Click **Save Changes**.

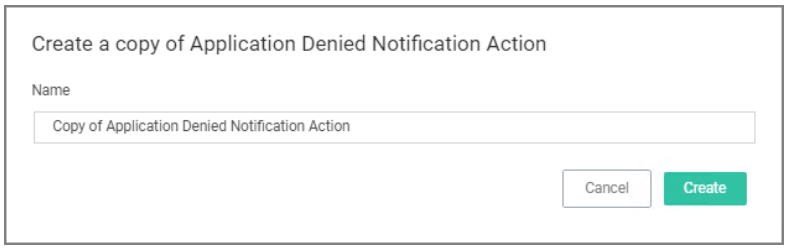
Customizing the Application Denied Notification Action

Default Actions shouldn't be edited directly, however Privilege Manager default items can be copied for customization purposes.

1. In the top Search box enter Application Denied Notification Action.
2. Click on the name of the Action **Application Denied Notification Action**.



3. Click **Duplicate**.
4. Enter a customized and meaningful name for the action. It is recommended to use standard naming conventions with your custom items. Beginning custom names with your company name is a great way to differentiate between the default items and your custom items.

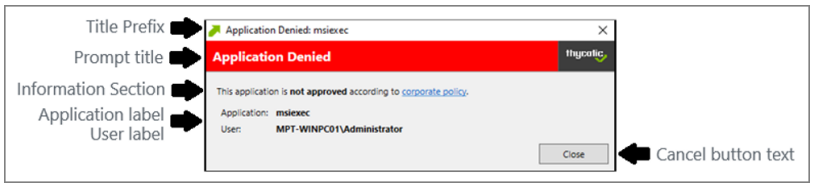


5. Click **Create**. Once you click Create, the new action page opens.
6. To upload a custom image file click **Choose File**. You can upload a custom logo, the file size should be under 128 KB and the width should be 500 pixels or less with a maximum hight of 34 pixels.

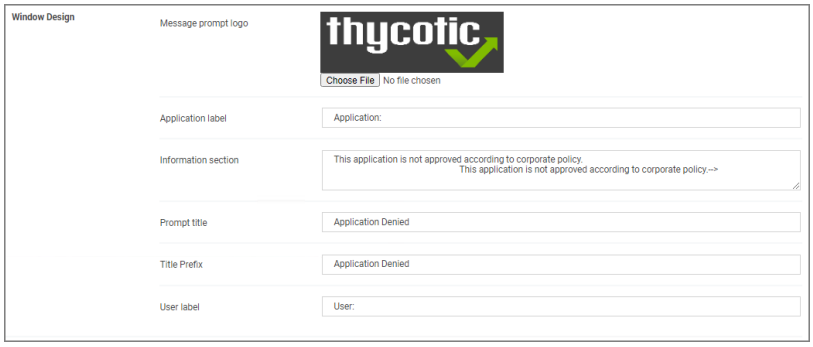
   The logo that is uploaded should NOT be a high-resolution image. This image will be delivered to every endpoint with every message in which it's used. The smaller the image, the better, for sending the message to the endpoints and for the endpoint to load the message.
7. Click **Save**.

Editing the Text in the UI

Privilege Manager makes it very easy to edit the text of a message. The fields are listed in alphabetical order on the item's view page. Compare each field to this overview image:



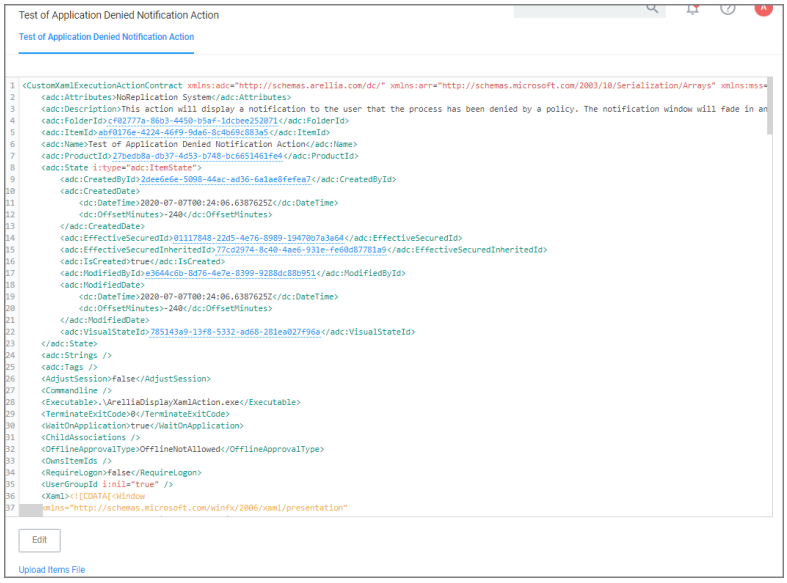
Most of the lines do not include individualized stylings per line. Editing the text in the UI will simply edit the text as required. The **Information Section** field includes html formatting for the hyperlink to the corporate policy. That hyperlink will be removed if the text is edited on the message's edit page.



Note: It is **NOT** recommended to edit the Information Section directly on the message's edit page. Instead, editing the Information Section via XML retains the html formatting for this line. If no changes are made to the Information Section, the html formatting is retained. All other fields can be changed except the Information Section and the html formatting for the Information Section is retained.

Editing the Text via XML

1. Select **More** an click **View as XML**.



2. Change the notification text in the XML viewer:

   Line 82 has the following:

```
<Paragraph><Run>This application is </Run><Bold><Run>not approved</Run></Bold><Run>
according to </Run><Hyperlink TargetName="_
blank" NavigateUri="http://www.example.com/policy"><Run>corporate
policy</Run></Hyperlink><Run>.</Run></Paragraph>
```

   Edit this space with the URL and the name of the Hyperlink you would like for your pop up Window.

```
<Paragraph><Run>This application HAS NOT BEEN APPROVED according to </Run><Hyperlink
TargetName="_blank" NavigateUri="http://www.example.com/policy"><Run>corporate
policy.</Run><Run>Click here, </Run><Hyperlink TargetName="_
blank" NavigateUri="http://www.thycotic.com/helpdesk"><Run>to open a support ticket for
review this application for approval.</Run></Hyperlink><Run>.</Run></Paragraph>
```

3. Change the default timeout:

   If you wish to change the default time out for how long the Deny Notification stays up (default is 6 seconds), edit Line 299:

```
<i:Interaction.Triggers>
<i:EventTrigger EventName="Loaded"><adx:InvokeCommandWithDelayAction
x:Name="CloseAction" Command="{BindingCloseCommand}" Delay="00:00:06"
/></i:EventTrigger></i:Interaction.Triggers>
```

   To change it to 15 seconds, edit this elements delay parameter to 15:

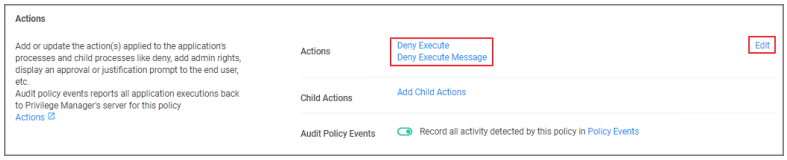
```
<adx:InvokeCommandWithDelayAction x:Name="CloseAction" Command="
{BindingCloseCommand}" Delay="00:00:15" />
```

4. Click **Import**. If you get an error, please address your changes. Errors are indicated with a red dot. Save any edits when resolving errors.

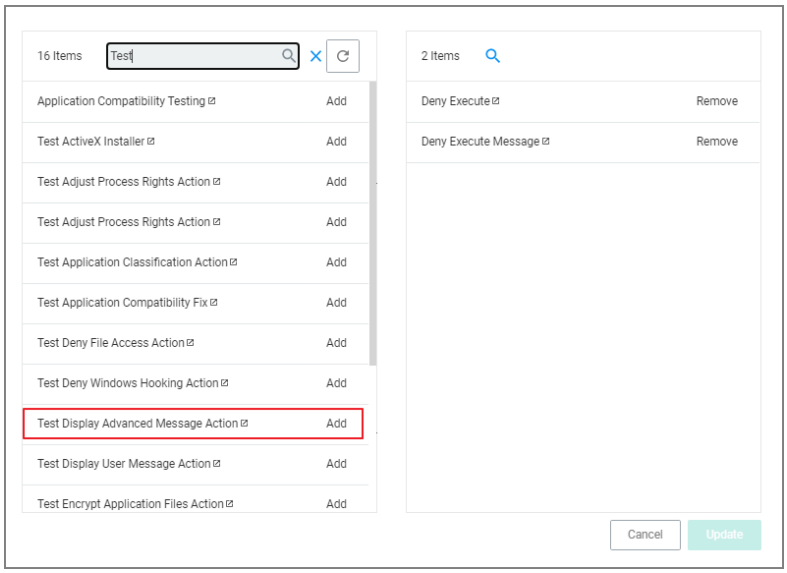
Updating the Policy with the new Action

After creating a custom notification action, the policy using the default notification needs to be updated.

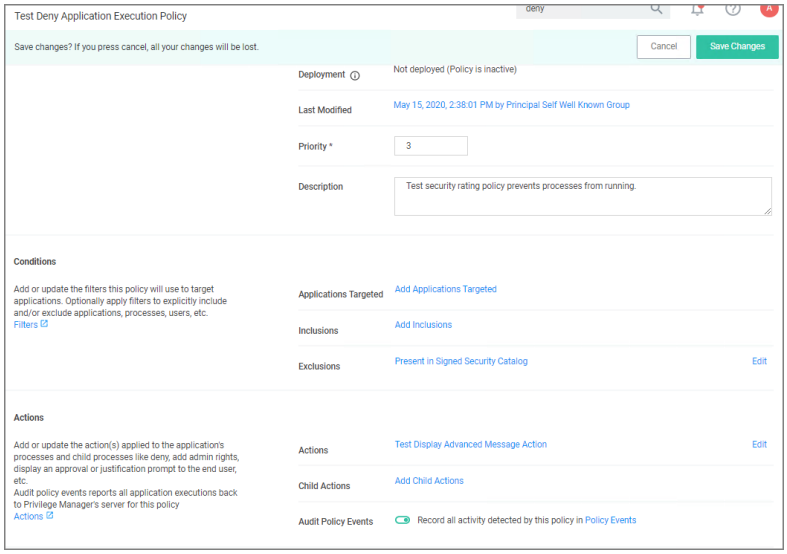
1. Navigate to **Application Policies** and locate the policy that uses the notification you wish to update.
2. Go to the **Actions** section.



3. Click **Edit**.
4. Search for the action you just duplicated and modified.



   a. Click **Add**, to add the action to the right pane of the dialog.
   b. Click **Remove** for the old action used previously.
5. Click **Update**.



6. Click **Save Changes**.

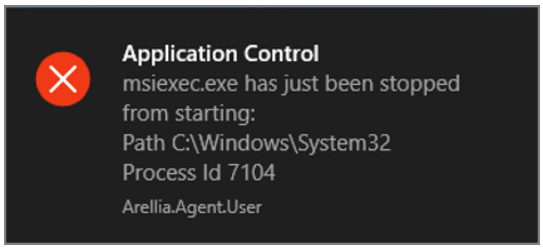
Policy changes are automatically propagated to the endpoints. Note, that this might not be instantaneous based on the refresh cycle.

Deny Execute Action

This action stops specific application from executing. It is a default action without any configurable settings. It is a read-only item.

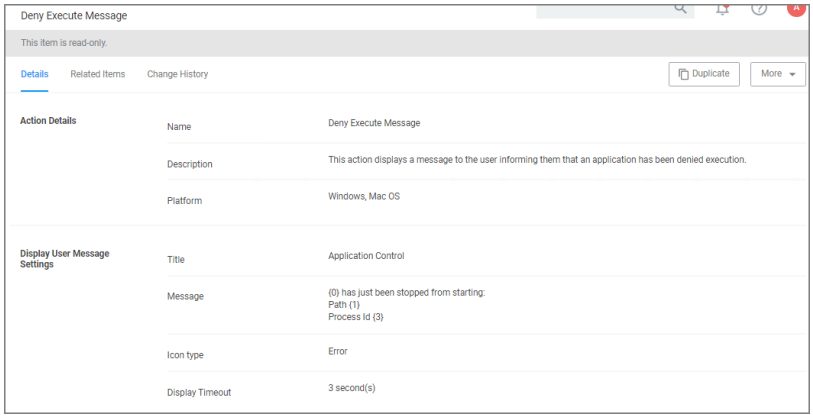
Deny Execute Message

This action displays a message to the user informing that an application has been denied execution. The Deny Execute Action needs to be used with this message.



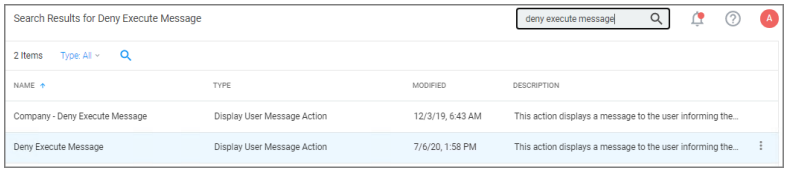
Deny Execute Message

The Deny Execute Message does not include company branding and is easy to edit in the Privilege Manager console. The default of this basic user message action is displayed like this:

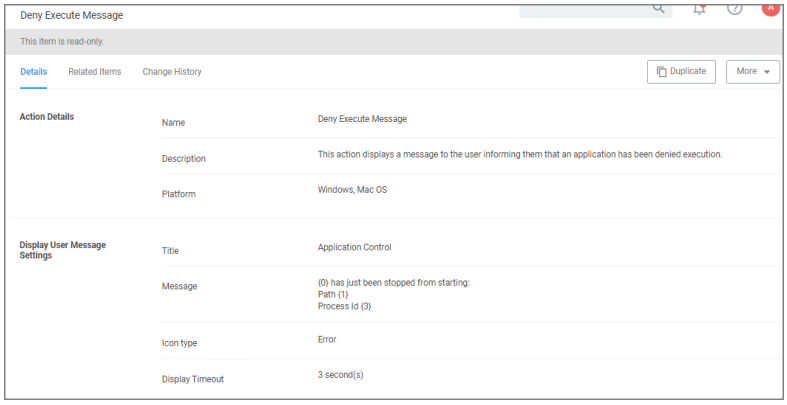


Customization

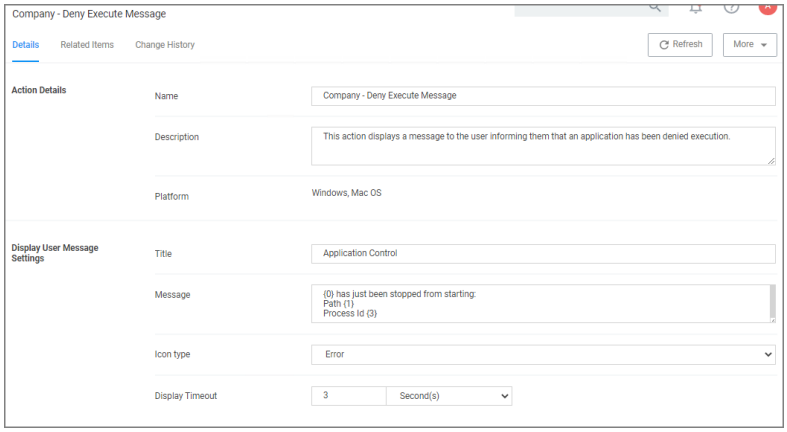
1. In Privilege Manager, search for the default message that will be customized. In this example, we search for the default **Deny Execute Message**.
2. Select the item from the search results.



3. This is a read-only action, to customize the default message, users need to click **Duplicate**.



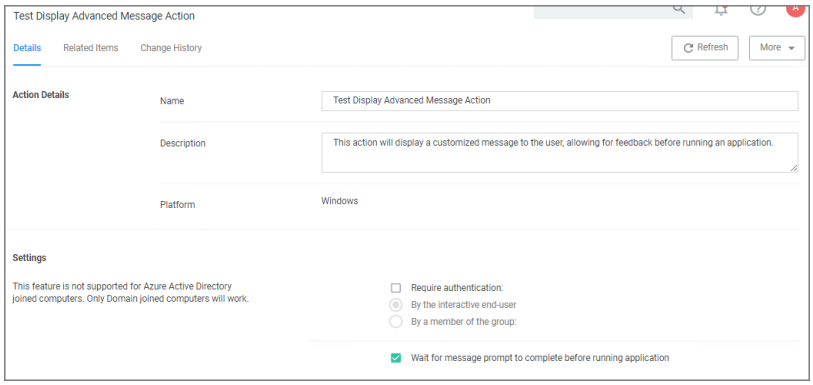
4. Enter a name for the new message action. It is recommended to use standard naming conventions with your custom items, e.g. beginning custom names with your company name is a great way to differentiate between the default items and your custom items.
5. Click **Create**.
6. Customize the Title and Message, use the Icon Type drop-down to specify the type, and set the Display Timeout.



7. Click **Save Changes**.

Display Advanced Message Action

Display messages are paired with another action type. They are customizable and serve to tell the end user what is happening and why. Advanced messages pop up in the middle of the screen, whereas Basic User messages appear as smaller pop-ups directly from the taskbar area.

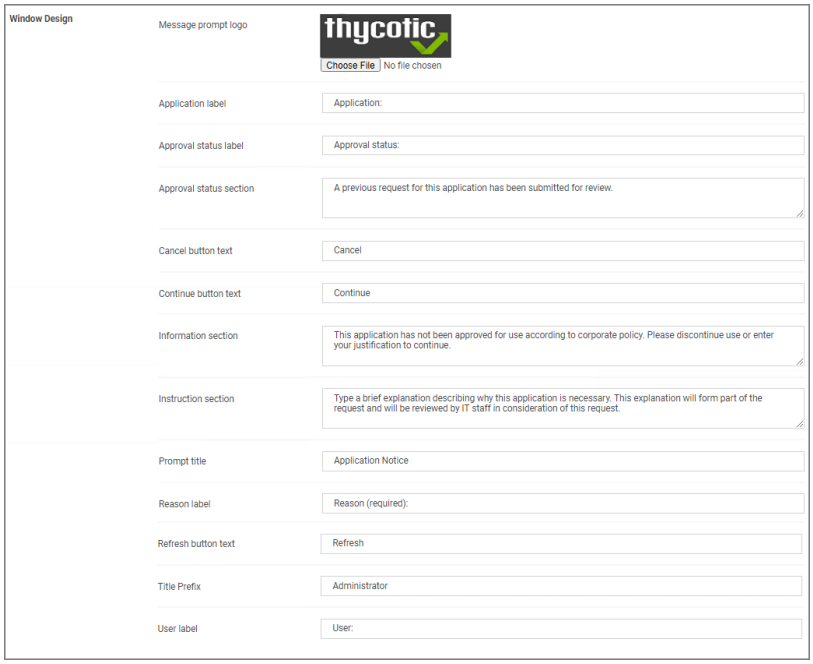


Parameters

The following Display Advanced Message Settings can be specified:

- Require authentication.
  - By the interactive end-user
  - By a member of the group
  - Wait for message prompt to complete before running application

Further the Window Design parameters can be set. Those settings include customization of company logo for branding, label, status, button, instruction, prompt, and reason texts just to name a view.

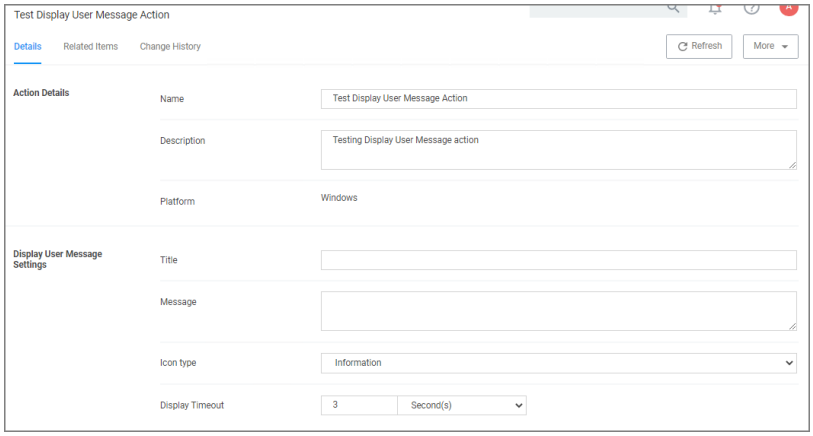


Examples

- Create Custom Notifications

Display User Message Action

Display messages are paired with another action type. They are customizable and serve to tell the end user what is happening and why. Advanced messages pop up in the middle of the screen, whereas Basic User messages appear as smaller pop-ups directly from the taskbar area.



This action is available for both Windows and macOS systems.

Parameters

The following Display User Message Settings can be specified:

- Title
- Message
- Icon type, which can be specified as Information, Warning, Error, Delinea, or Program.
- Display timeout setting, which can be specified in Seconds, Minutes, Hours, Days, or Weeks.

Examples

- Deny Execute Message

macOS Specific Actions

The following are macOS specific topics on actions:

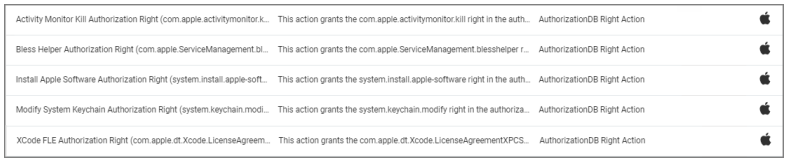
- Allow Copy Action (macOS)
- AuthorizationDB Right Actions
- Command Line Approval Message
- Command Line Justification Message Action
- Display Advanced User Message Action (macOS)
- Just-in-Time Group Membership Action

- Run as User Action
- WYSIWYG macOS Action Message Editor

AuthorizationDB Right Actions

Privilege Manager provides the following default AuthorizationDB Right actions:

- Activity Monitor Kill Authorization Right (com.apple.activitymonitor.kill)
- Bless Helper Authorization Right (com.apple.ServiceManagement.blesshelper)
- Install Apple Software Authorization Right (system.install.apple-software)
- Modify System Keychain Authorization Right (system.keychain.modify)
- Xcode FLE Authorization Right (com.apple.dt.Xcode.LicenseAgreementXPCServiceRights)

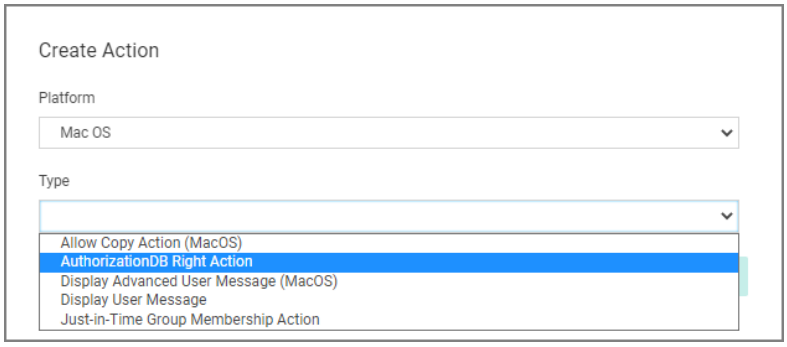


Activity Monitor Kill Authorization Right (com.apple.activitymonitor.k...	This action grants the com.apple.activitymonitor.kill right in the auth...	AuthorizationDB Right Action
Bless Helper Authorization Right (com.apple.ServiceManagement.bl...	This action grants the com.apple.ServiceManagement.blesshelper r...	AuthorizationDB Right Action
Install Apple Software Authorization Right (system.install.apple-soft...	This action grants the system.install.apple-software right in the auth...	AuthorizationDB Right Action
Modify System Keychain Authorization Right (system.keychain.modi...	This action grants the system.keychain.modify right in the authoriza...	AuthorizationDB Right Action
XCode FLE Authorization Right (com.apple.dt.Xcode.LicenseAgreem...	This action grants the com.apple.dt.Xcode.LicenseAgreementXPCS...	AuthorizationDB Right Action

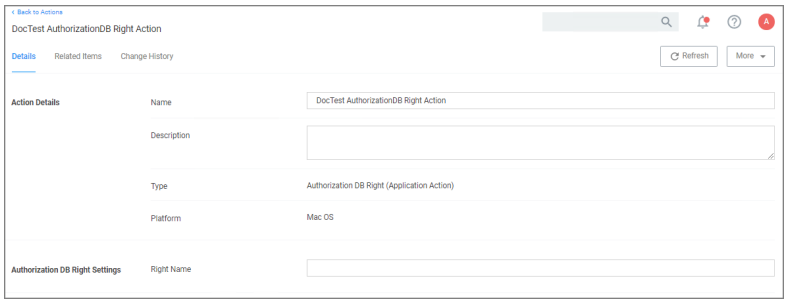
Privilege Manager AuthenticationDB actions should not be used with advanced message actions such as Approval, Deny, Justification, or Warning should not be used in conjunction with this action.

Creating a Custom AuthorizationDB Right Action

1. Navigate to **Admin | Actions**.
2. Click **Create Action**.
3. From the **Platform** drop-down select **macOS**.
4. From the **Type** drop-down select **AuthorizationDB Right Action**.



5. Enter a name, that allows you to easily identify the action for future use.
6. Click **Create**.



7. Under Authorization DB Right Settings in the **Right Name** field enter the desired authorization database right name.
8. Click **Save Changes**.

The action can now be added to existing macOS elevation policies or selected at policy creation following the use of **Modify Authorization Right** on the final create policy wizard page by selecting it from the **Right Name** drop-down.

Refer to the following examples:

- Elevating Xcode
- Elevating Modifying the Keychain
- Elevating Charles Proxy
- Elevating Activity Monitor

Command Line Approval Message Action

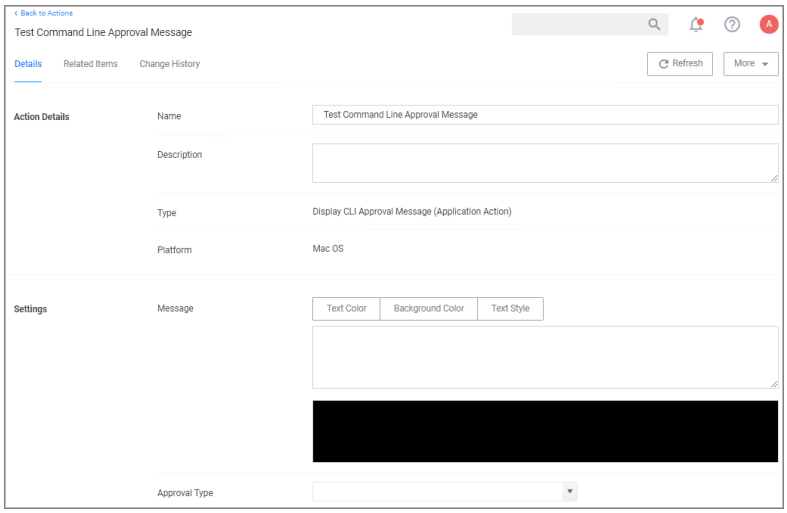
The Command Line Approval Message action allows administrators to prompt command line users on macOS endpoints for an approval request. The action displays text in the command line interface and prompts the user to enter text.

This action is specifically designed to work with the Delinea macOS sudo plugin and is only intended for commands that run under `sudo` based on the following use case:

- the user runs `sudo <command>`
- the user is prompted to supply a justification, which happens directly in the same terminal
- the command is then run with elevation

To create the message action,

1. Navigate to **Admin | Actions**.
2. Click **Create Action**.
3. For **Platform**, select **macOS**.
4. For **Type**, select **Command Line Approval Message**.
5. Enter a name and description.
6. Click **Create**.



7. Under **Settings** for:
   - **Message**, use the color tooling options and editor to add and customize your message prompt for the users.
   - **Approval Type**, from the drop-down select either
     - **Default Execute Application Request Type** or
     - **Default Offline Execute Application Request Type**.
8. Click **Save Changes**.

Refer to Using the Command Line Action Editor for information on how to use the editor.

> **Note:** The Command Line Approval Message action is the preferred message action to elevate commands and scripts run under `sudo` requiring approval.

If there are networking issues, while a CLI approval is being used, the following error might be displayed in Terminal: *Error occurred in policy engine*. This is due to offline CLI approvals not being supported at this time.

Command Line Justification Message Action

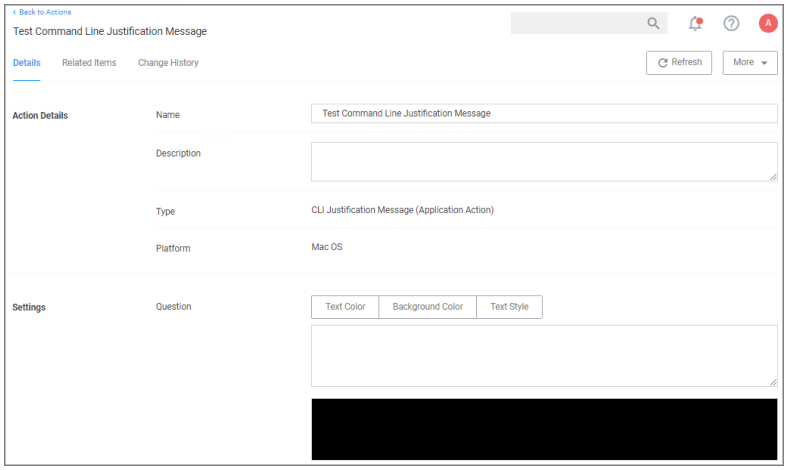
This message action prompts the user for a justification when using Terminal to execute commands and scripts under `sudo`. This action is specifically designed to work with the Delinea macOS sudo plugin and is only intended for commands that run under `sudo` based on the following use case:

- the user runs `sudo <command>`
- the user is prompted to supply a justification, which happens directly in the same terminal
- the command is then run with elevation

To create the message action,

1. Navigate to **Admin | Actions**.
2. Click **Create Action**.
3. For **Platform**, select **macOS**.

4. For **Type**, select **Command Line Justification Message**.
5. Enter a name and description.
6. Click **Create**.



7. Under Settings, use the color tooling options and editor to add and customize your message prompt for the users.
8. Click **Save Changes**.

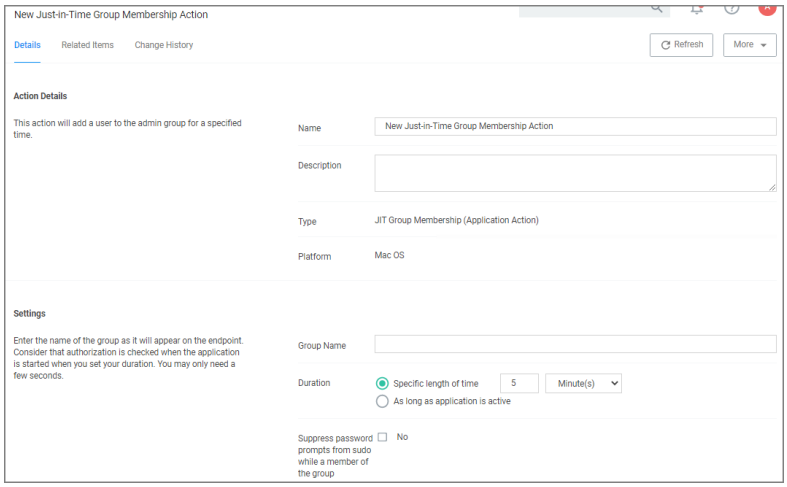
Refer to Using the Command Line Action Editor for information on how to use the editor.

> **Note:** The Command Line Justification Message action is the preferred message action to elevate commands and scripts run under `sudo`.

Just-in-Time Group Membership Action

This action will add a user to the specified group for a specified time. This action can then be added to a controlling policy to give Just-in-Time elevation to a user. The action is a read-only action by default. To customize this macOS action for your endpoints, use the **Duplicate** option.

1. Navigate to **Admin | Actions**.
2. Search for and select **Just-in-Time Group Membership** from the list of available macOS actions.
3. Click **Duplicate**.
4. Enter a name for your newly created action and click **Create**.



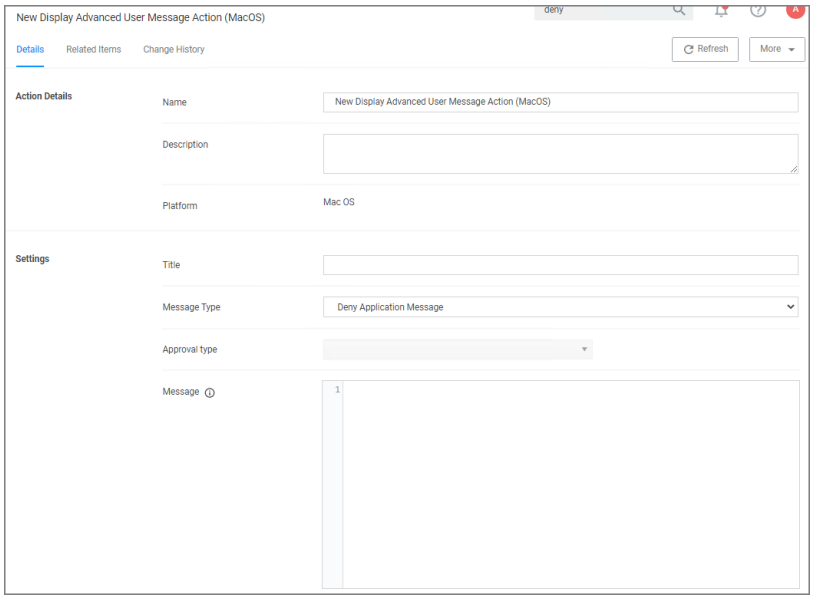
5. Under **Settings** specify
   a. the **Group Name** as created on the endpoint.
   b. the **Duration** either
      - set a specific length of time, here you need to consider that authorization is started when the application starts, or
      - use the default *as long as application is active*.
   c. enable the **Suppress password prompts from sudo while a member of the group** if the user should **not** be prompted for the standard user password while in the group.
6. Click **Save Changes**.

> **Note:** The *Suppress password prompts from sudo while a member of the group* checkmark is intended for use with scripts that may execute multiple sudo commands, such as the Homebrew installer.

Refer to the topic macOS Homebrew Installer Support for details on the policy setup.

Display Advanced User Message Action (macOS)

Display messages are paired with another action type. They are customizable and serve to tell the end user what is happening and why. Advanced messages pop up in the middle of the screen, whereas Basic User messages appear as smaller pop-ups directly from the taskbar area.



Parameters

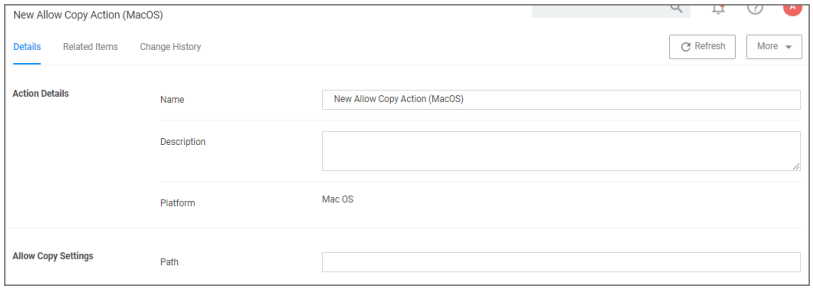
The following Display Advanced Message Settings can be specified:

- Title
- Message Type, such as
  - Deny Application Message
  - Warning Message
  - Justify Application Usage
  - Deny Application with Justification
  - Approval Request Message
- Message, which is the actual text of the message displayed to the user.

Allow Copy Action (macOS)

Important: This action will not work with v11.2+ macOS agents.

Action to allow copying of application on macOS systems.



Parameters

The following Allow Copy Action Settings can be specified:

- Path

Run as User Action

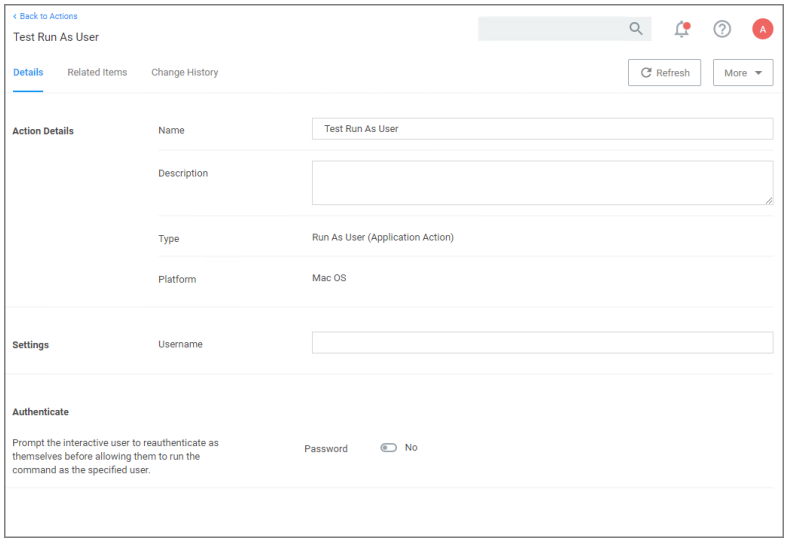
The action specifies the username of the account under which to run a command when invoked by 'sudo'.

For example, the `/usr/bin/id` command prints the current account's username. If a policy is created to match this command with an action that specifies a particular username, then entering "sudo id" will run the "id" command as that user and it will display that username.

The account must already exist on the endpoint, or `sudo` will display an error message and exit without running the command.

To create the message action,

1. Navigate to **Admin | Actions**.
2. Click **Create Action**.
3. For **Platform**, select **macOS Computers Actions**.
4. For **Type**, select **Run as User**.
5. Enter a name and description.
6. Click **Create**.



7. Under **Settings** for **Username**, specify as which user to run the command.
8. Under **Authenticate** you may change the switch to require a password. The default is to run the command as the specified user without prompting for a password.

   When the password prompt is enabled, `sudo` first prompts for the password of the **logged-in user** before running the command as the specified user. In addition, the action can specify a time interval during which the user will

not be re-prompted for their password when running the command targeted by the policy that contains the action.

9. Click **Save Changes**.

Time Interval Retention

By default, `sudo` retains the user's authentication for 5 minutes, but different actions can have different intervals. Continuing the example above, if the user runs `sudo -k` followed by `sudo id`, which clears the sudo credential cache, the `sudo` plugin resets the interval for any Run as User action active for that user. `sudo -k` followed by `sudo id` will prompt the user for their password regardless of whether the specified interval has passed, and it will apply to any other command governed by a run-as-user policy.

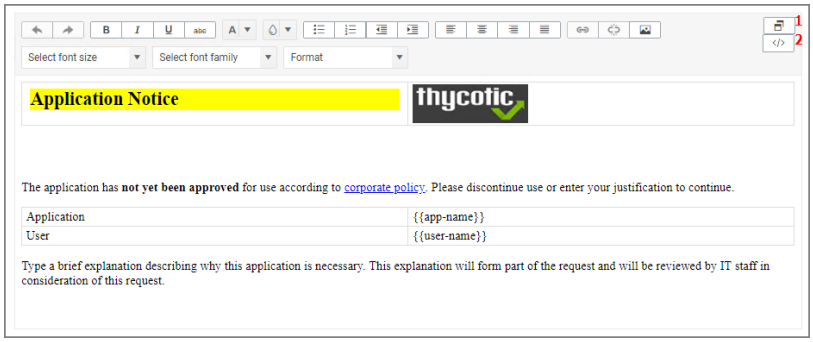
WYSIWYG macOS Action Message Editor

All macOS based Display Advanced Message Action types are supported via an WYSIWYG editor for user friendly editing of advanced message action text. Any HTML based message can be rendered by the Agent on the macOS endpoint.

The editor is currently available for the following actions:

- Application Approval Request (with Offline Fallback) Message Action
- Application Approval Request (with ServiceNow Request Item Number) Message Action
- Application Approval Request Message Action
- Application Denied Message Action
- Application Justification Message Action
- Application Warning Message Action

Actions are read-only and a duplicate needs to be created before any customized message action can be created. Once you create a duplicate, you will see the following under **Settings | Message**:



Where:

- [1] is the undock button, which allows you to edit the page in full-size view.
- [2] is the source toggle, which allows you to edit the HTML source for the message action.

The editor comes with various style element options to further simplify the message editing process.

Edit any of the message elements for your users on your endpoints, except for the app-name and user-name variables. Those are system derived.

Any message action should be tested in light and dark mode before populating to endpoints.

Note: You can upload a custom logo, the file size should be under 128 KB and the width should be 500 pixels or less with a maximum hight of 34 pixels.

The logo that is uploaded should NOT be a high-resolution image. Consider that this image will be delivered to every endpoint with every message in which it is used. The smaller the image, the better, for sending the message to the endpoints and for the endpoint to load the message.

Unix/Linux Specific Actions

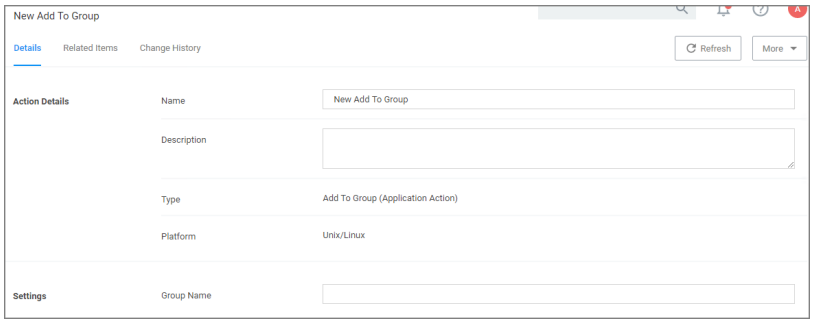
Note: Privilege Manager for Linux/Unix and Windows for servers is End of Sale/Renewal only.

The following Unix/Linux specific action topics are available:

- Add to Group Action
- Adjust Environment Variable Action
- Command Line Justification Message
- Command Line Approval Message
- Display User Message Action
- Run As User Action

Add to Group Action

The Add to Group action provides group membership to the running process via policy for temporary access.

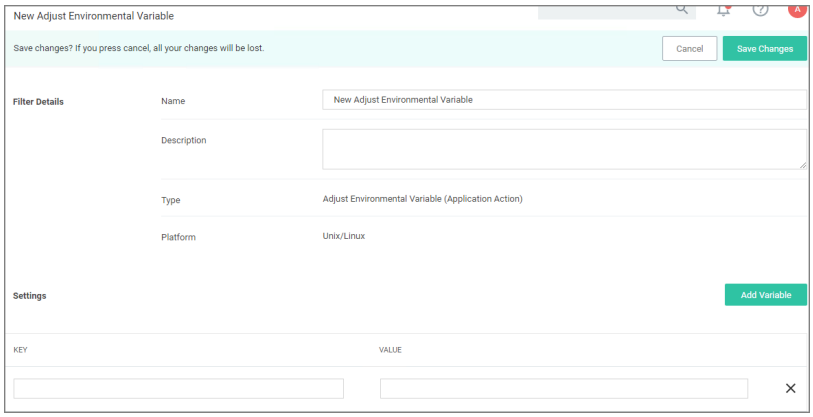


Settings

- Group Name: Specifies the Group Name for the temporary access.

Adjust Environment Variable Action

The Adjust Environment Variable action is used to customize environment variables on an endpoint.



Settings

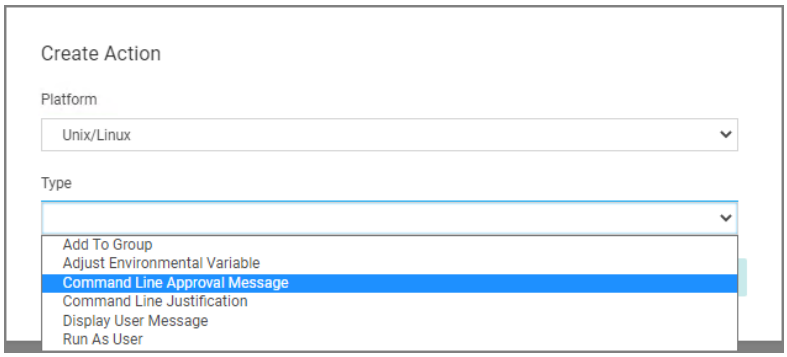
- Add Variable: Administrators can add and/or edit one or more variable key:value combinations.

Command Line Approval Message Action

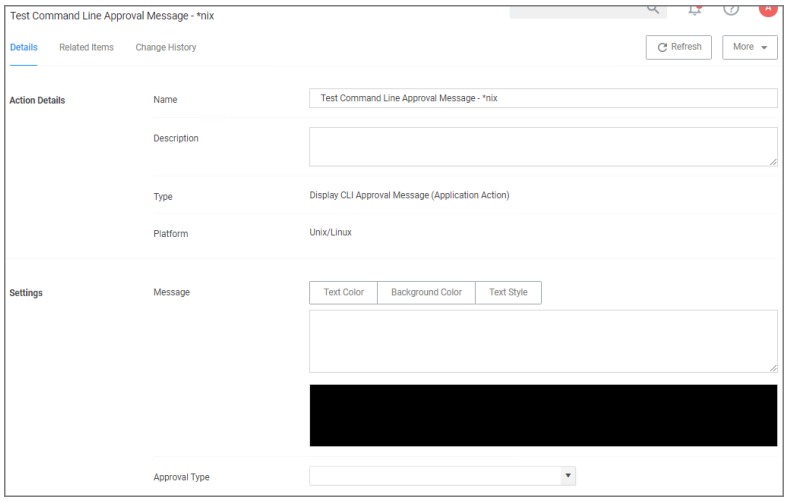
The Command Line Approval Message action allows administrators to prompt command line users on Unix/Linux endpoints for an approval request. The action displays text in the command line interface and prompts the user to enter text.

To create the message action,

1. Navigate to **Admin | Actions**.
2. Click **Create Action**.



3. For **Platform**, select **Unix/Linux**.
4. For **Type**, select **Command Line Approval Message**.
5. Enter a name and description.
6. Click **Create**.



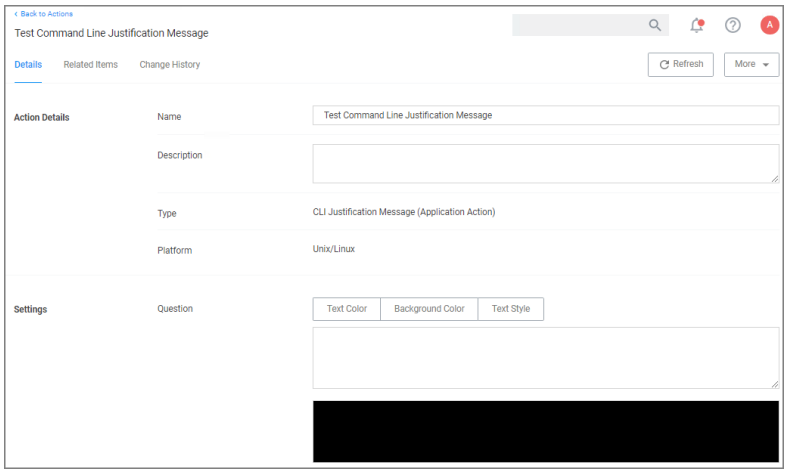
7. Under **Settings** for:
   - **Message**, use the color tooling options and editor to add and customize your message prompt for the users.
   - **Approval Type**, from the drop-down select either
     - **Default Execute Application Request Type** or
     - **Default Offline Execute Application Request Type**.
8. Click **Save Changes**.

Refer to Using the Command Line Action Editor for information on how to use the editor.

Command Line Justification Message Action

The Command Line Justification Message action can be used to provide a customized multi-line justification question to the user.

1. Navigate to **Admin | Actions**.
2. Click **Create Action**.
3. For **Platform**, select **Unix/Linux**.
4. For **Type**, select **Command Line Justification Message**.
5. Enter a name and description.
6. Click **Create**.

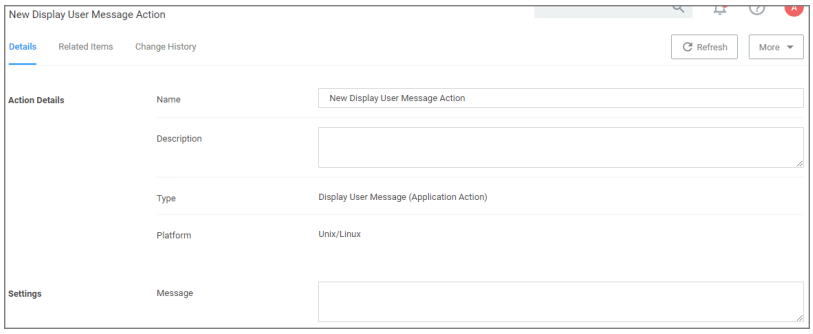


7. Under **Settings**, use the color tooling options and editor to add and customize your message prompt for the users.
8. Click **Save Changes**.

Refer to Using the Command Line Action Editor for information on how to use the editor.

Display User Message Action

The Display User Message action provides the option of a customized user message to be displayed to the user at an endpoint.

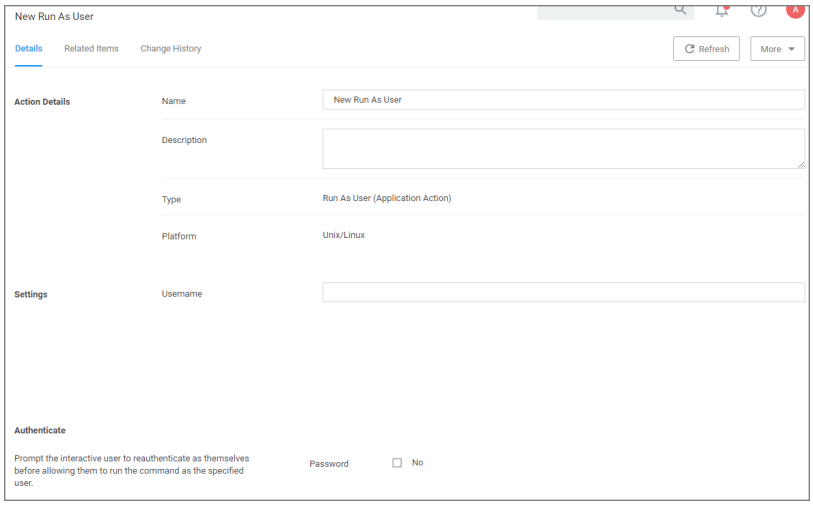


Settings

- Message: Multi-line text field for a customized message to be displayed at an endpoint.

Run as User Action

This actions allows a command a user runs on an endpoint to be treated as if a different user ran it.



Settings

- Username: This identifies the username under which to run the command at the endpoint.

Authenticate

By default, the system requires the user to authenticate themselves, before they are allowed to run a command as the specified user. This can be changed by setting the password prompt to off, and thus disabling the re-authentication.

Windows Specific Actions

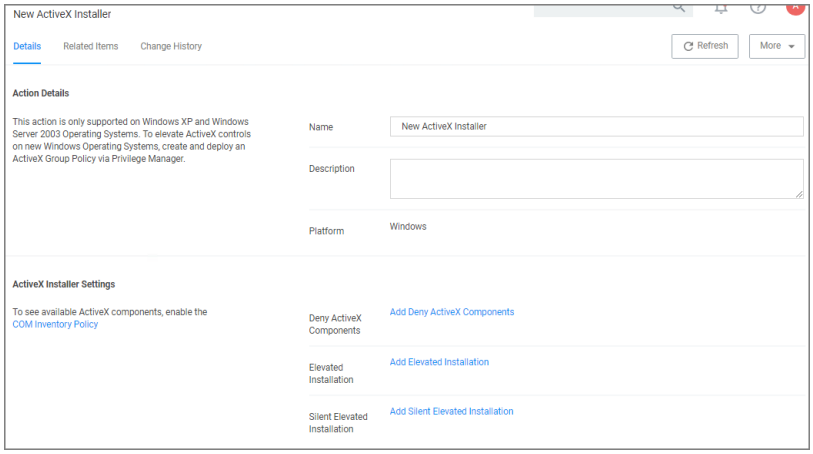
The following are Windows specific topics on actions:

- ActiveX Installer Action
- Application Classification Action
- Apply Application Compatibility Fix Action
- Deny File Access Action
- Deny Windows Hooking Action
- "Microsoft Entra ID Authentication" on page 506
- Encrypt Application Files Action
- Endpoint Group Member Approval Action
- Set Environment Variable Action
- Execute Application Action
- Group Member Approval Action
- Sandbox Action
- Set Process Security Descriptor Action

- Adjust Process Rights Action
- WYSIWYG Windows Action Message Editor

ActiveX Installer Action

This type of action is a specific use-case for older Windows systems (Windows XP and Windows Server 2003). The ActiveX installer action allows or denies an application to enable standard users to install approved ActiveX components. If you don't know what ActiveX means, you won't need to use this type of action.



Parameters

The following details can be set on the ActiveX action:

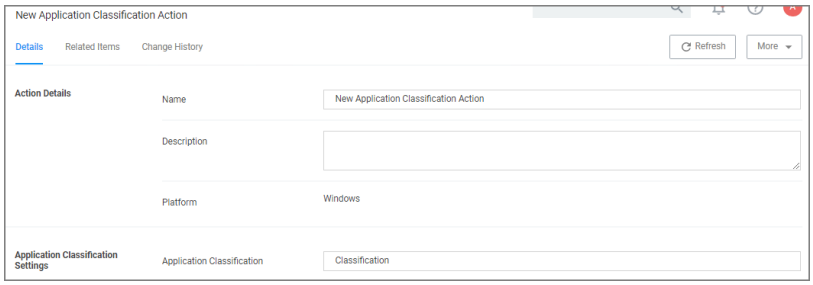
- Deny ActiveX Components, or
- Elevated Installation, or
- Silent Elevated Installation

For those actions for ActiveX, these parameters can be specified:

- Scope by Organization Group
- Search text
- Maximum rows returned
- Resources (use the column filter function to locate a resource and click **Add**)

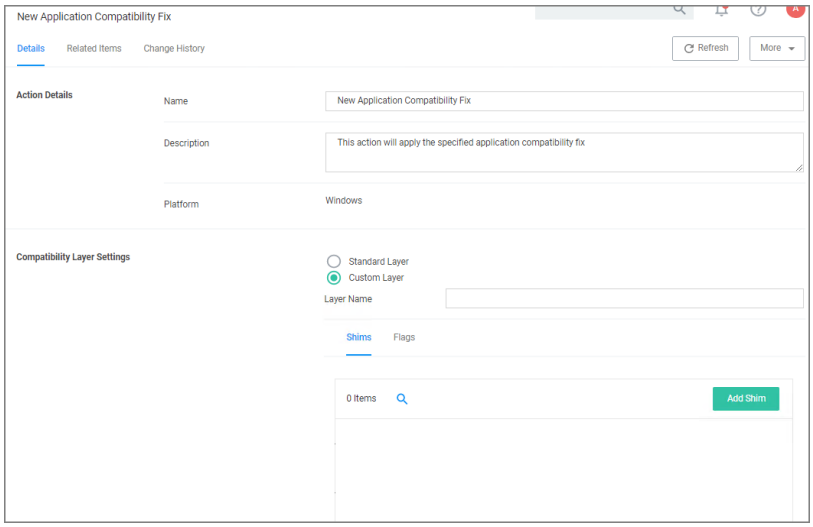
Application Classification Action

This type of action will restrict applications from modifying certain items and will enforce standard Windows ACLs when the targeted application accesses restricted files, folders, registry keys, or services on a computer.



Apply Application Compatibility Fix Action

This type of action will allow old applications that must be run via compatibility mode to execute without manual compatibility adjustments.



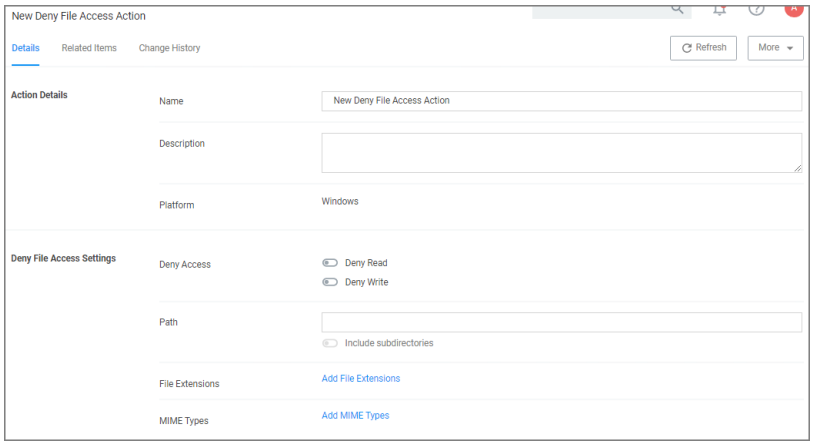
Parameters

The following Compatibility Layer Settings can be set on the Apply Application Compatibility Fix action:

- Custom vs. Standard Layer, which lets users select a layer either x86 and x64, x86 only, or x64 only.
- Shims
- Flags

Deny File Access Action

As the name suggests, this type of action will prevent applications from reading or writing (or both) to certain directories or to certain file types.



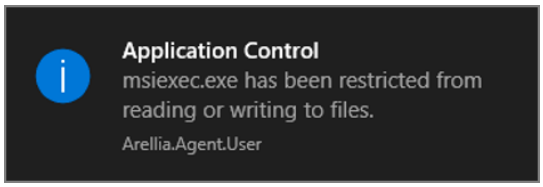
Parameters

The following Deny File Access Settings can be specified:

- Deny Access to read and/or write operations.
- Path and possibly subdirectory locations.
- Specific file extensions.
- MIME types.

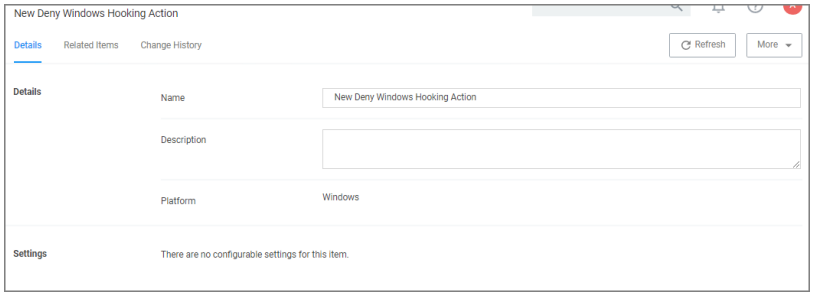
Deny Files Read and Write Access Message

This action displays a message to the user informing that an application will be restricted from certain file access. The Deny Read/Write Access to Microsoft Office Document Files Action needs to be used with this message.



Deny Windows Hooking Action

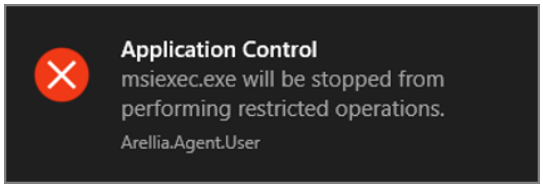
This type of action will limit specified applications from interacting in malicious ways with other applications.



This action does not have any configurable parameters.

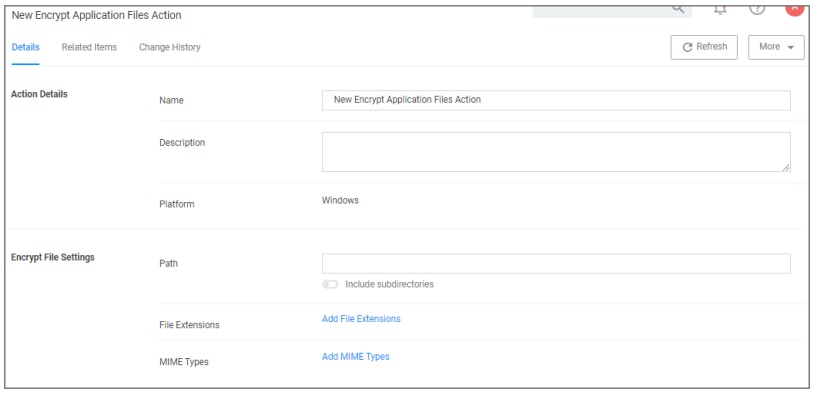
Windows Hooking Message

The action displays a message to the user informing them that an application will be stopped from interacting with other applications. The Deny Windows Hooking Action should be used with this message.



Encrypt Application Files Action

This type of action will force applications to use Microsoft encryption when saving a file.



Parameters

The following Encrypt Application Files Settings can be specified:

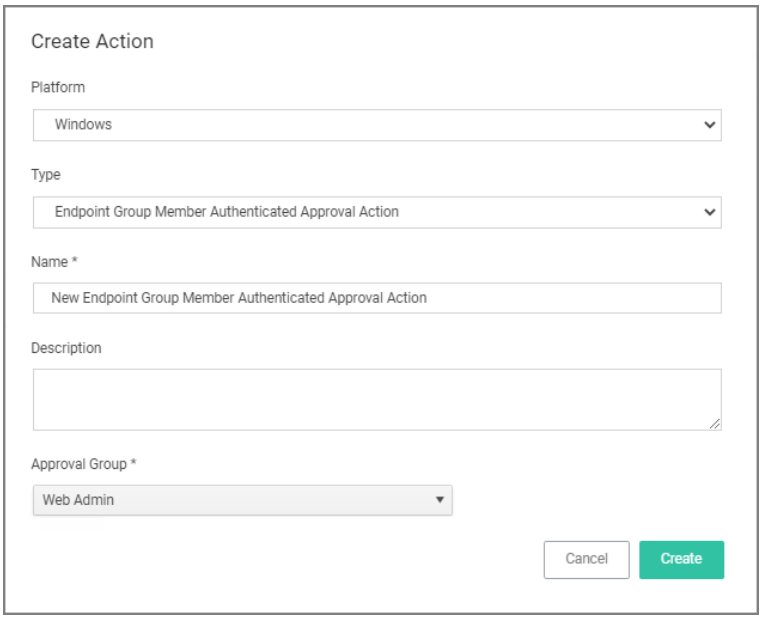
- Path and the option to include subdirectories.
- File Extensions.
- MIME Types.

Workstation Group Member Approval Action

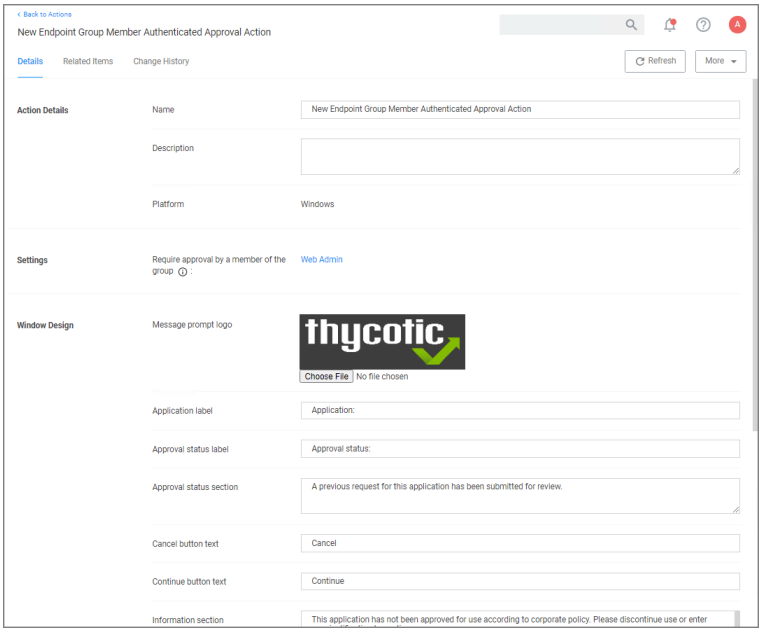
This action can be used for *over the shoulder* approvals, whether systems are on- or offline. The supervisor approves access by authentication on the user's workstation.

1. Navigate to **Admin | Actions**.
2. Click **Create**.
   a. On the **Create Action** modal from the **Platform** drop-down select **Windows**.
   b. From **Type** drop-down select **Endpoint Group Member Authenticated Approval Action**.
   c. Enter a meaningful **Name** and **Description**.

d. From the **Approval Group** drop-down, select the group membership of the approver.



e. Click **Create**.

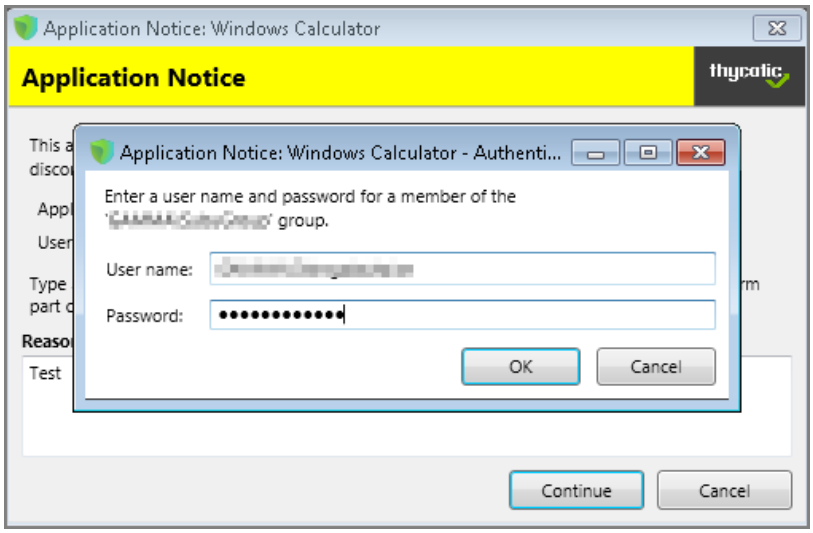


3. Under Settings verify the **Require approval by a member of the group:** contains the correct group. If you ever need to change it, come back to this page and click the group name to access the change modal.
4. Navigate to your computer group's **Application Policies**, click **Create Policy** or find an existing policy that you want to use for these approvals.
5. Under the **Actions** section, search for and add the action you previously created.

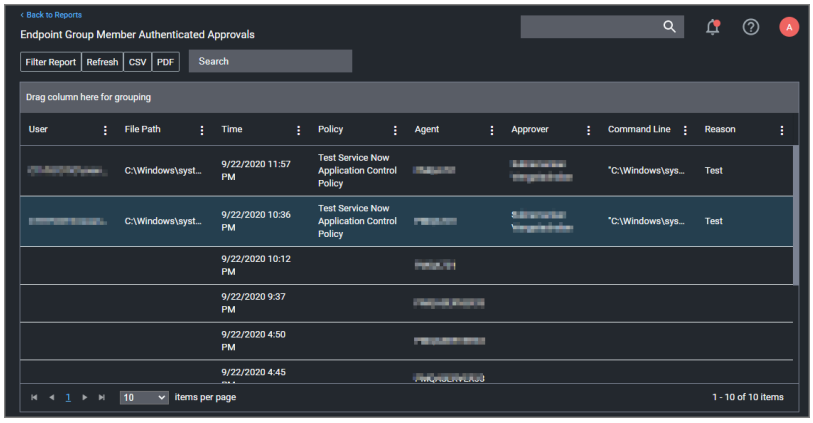
6. Click **Save Changes**.
7. Click the **i** next to **Deployment** and select **Resource and Collection Targeting Update** to immediately send the policy to your workstation agents.

Policies also automatically update according to a schedule.

Sample Group Member approval notice with approval overlay:



Refer to the **Endpoint Group Member Authenticated Approvals** report to view a history of "over the shoulder" approvals:

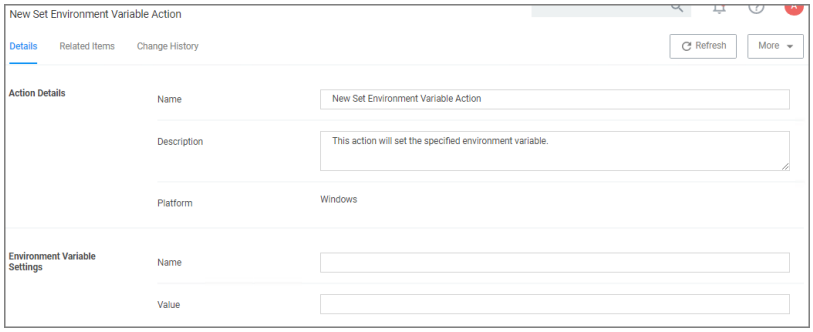


Related Topics

- Group Member Authenticated Message Action, which guides you through setting up approvals based on the group membership of the approver.
- Using an Endpoint Group Member Authenticated Message Action, which guides you through setting up *over the shoulder* approvals that can be used on- and offline with a ServiceNow system integration.

Set Environment Variable Action

This type of action sets an environment variable for processes that could change the behavior of an application, or be caught by an Environment Variable filter in another policy.

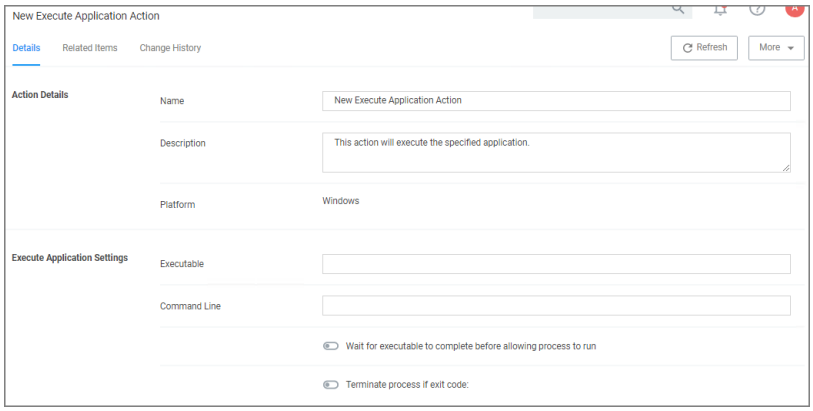


Parameters

The parameters for the Set Environment Variable action are setting the name and value of the environment variable.

Execute Application Action

This type of action will execute another application and (optionally) wait on that process to complete before the original process can execute.



Parameters

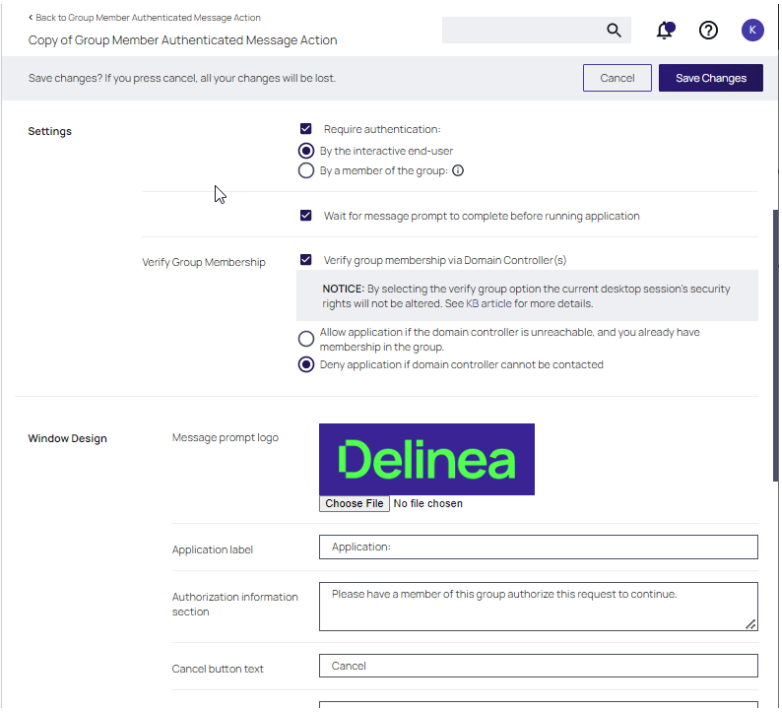
The following Execute Application Settings can be specified:

- an executable
- command line arguments

Group Member Approval Action

This action can be used for approvals that are based on a group membership authentication of the approver.

1. Navigate to **Admin | Actions**.
2. Search and select **Group Member Authenticated Message Action**.
3. Click **Duplicate**.
4. Name your new action and click **Create**.



5. Customize the Action based on your specific business requirements.
6. Verify the **By the member of the group:** is active and a group is listed below the button. If you ever need to change it, come back to this page and click the group name to access the change modal.
7. Determine the state of the **Verify group membership via Domain Controller(s)** check box.

   Note: This option relies on the ability of computers to contact their domain controllers in real time to authenticate users and refresh group memberships.

   If enabled, the Delinea agent will contact a domain controller to re-authenticate the user and refresh group memberships each time this action is invoked. If a domain controller cannot be contacted, authentication will be controlled by the **Verify Group Membership** radio buttons.

   If disabled, the Delinea Agent will use the group membership information that is present in the user's desktop session, which reflects the group memberships that were in effect when the user logged on to their desktop and may no longer be accurate.
8. Click **Save Changes**.
9. Navigate to your computer group's **Application Policies**, click **Create Policy** or find an existing policy that you want to use for these approvals.

10. Under the **Actions** section, search for and add the action you previously created.
11. Click **Save Changes**.
12. Click the **i** next to **Deployment** and select **Resource and Collection Targeting Update** to immediately send the policy to your endpoint agents.

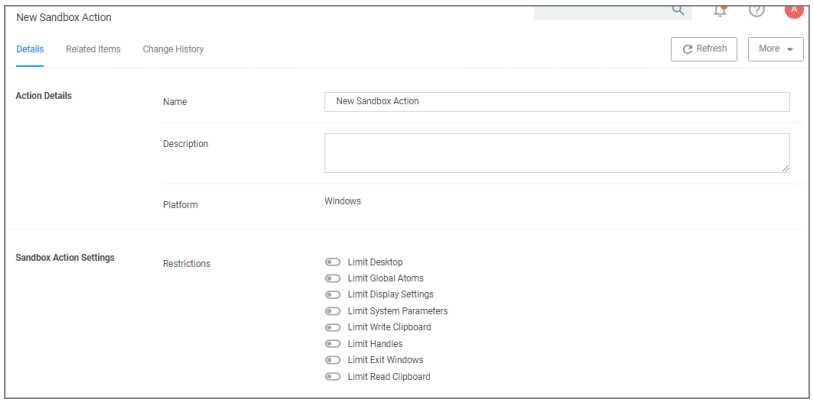
Policies also automatically update according to a schedule.

Related topics:

- Endpoint Group Member Authenticated Message Action, which guides you through setting up *over the shoulder* approvals that can be used on- and offline.
- Using an Endpoint Group Member Authenticated Message Action, which guides you through setting up *over the shoulder* approvals that can be used on- and offline with a ServiceNow system integration.

Sandbox Action

This type of action will limit the environments in which certain code can execute. The sandbox runs a process in a job object that limits its ability to interact with other processes, as well as limiting some specific types of interactions with the operating system.



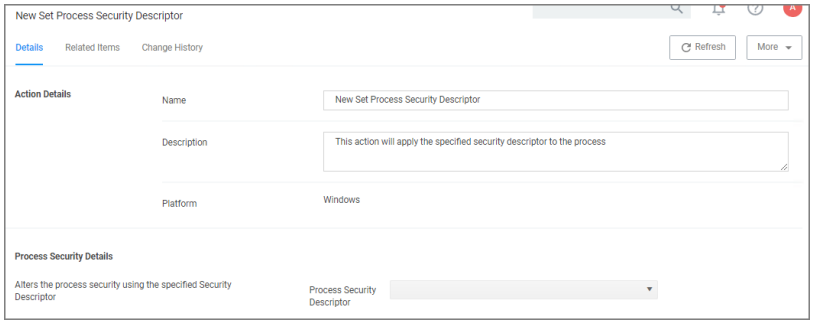
Parameter

The following Sandbox Action Settings can be enabled:

- Limit Desktop
- Limit Global Atoms
- Limit Display Settings
- Limit System Parameters
- Limit Write Clipboard
- Limit Handles
- Limit Exit Windows
- Limit Read Clipboard

Set Process Security Descriptor Action

Adjusting Process Security allows a process to be protected from most tampering by users. For example, adjusting process security can restrict who can stop a process from the task manager.



Parameters

The parameters for the Set Process Security Descriptor action are done via resource selection from a list of available security descriptors.

Adjust Process Rights Action

This topic explains the Adjust Process Rights Action and Unrestricted Tokens in Privilege Manager.

When elevating process rights with Application Control Solution (ACS) on Windows, there are times when the rights given by ACS appear to be insufficient. The process still doesn't work as it does when the user is logged in as Administrator, accepts the UAC box, or the process is run with the right-click Run As Administrator option. Sometimes an error is returned stating insufficient rights to access.

Microsoft with the release of Windows Vista introduced changes to security which included creating two tokens for users when they log in. For more information refer to the Microsoft Documentation on Restricted Tokes.

The lower privilege token is the one always used unless the user goes through UAC or other processes. ACS allows administrators to choose which token should be used to elevate certain processes. The lower privilege token, if it works, is the better option as it has fewer privileges and thus protects the system better. But if necessary, the higher-privilege token can be used by ACS when manipulating the process's security configuration.

The following are the Privilege Manager default Adjust Process Rights Actions. As with all actions delivered with Privilege Manager, these actions cannot be modified. They can be copied and then customized and as many actions as necessary can be created for a custom implementation:

- Add Administrative Rights
- Add Administrative Rights - Unrestricted
- Adjust Process Rights for Resource Monitor
- Remove Administrative Rights
- Remove Advanced Privileges Action

Each of those actions has by default Related Items associated, which need to be considered when customizing an action.

Note: The **Suppress UAC Consent Dialog (Legacy)** action should only be used with Agent versions 10.4 and older.

Adjust Process Rights Action Settings Explained

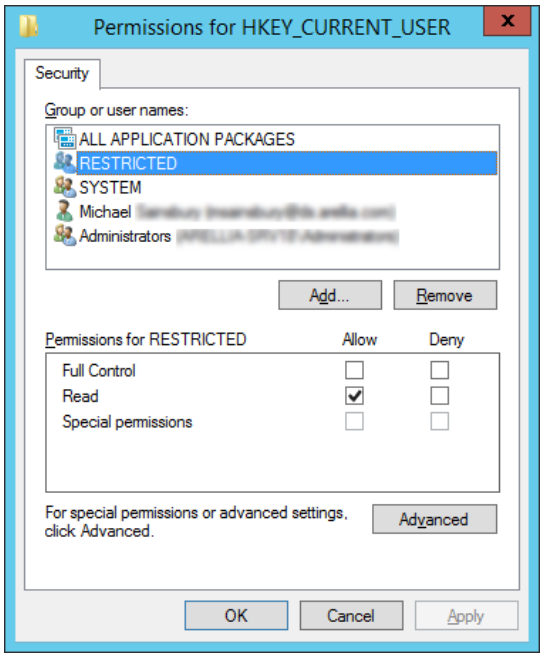
The application action elevates or restricts the permissions and/or privileges held by a process security token. By default, each process inherits the user's security token.

The four main areas to customize are:

- Selecting an **Action Type**, which can either Elevate Rights or Restrict Rights. When the adjustment is a rights restriction, there is an advanced feature that allows you to apply restricted Security Identifiers (SIDs), which further restricts access to securable objects. More about this under the What is a Restricted SID topic.
- Adding or Removing **Windows Privileges**, these come pre-populated with a set of default recommendations for each out of the box Action. To learn more about these Windows Privileges visit Microsoft's Documentation about User Rights Assignment.
- Adding or Removing **Build-in Roles**, these are the roles that provide file level access to a system and they are based on group membership.
- Adding or Removing **Well-known Accounts**, these are specifying the integrity levels at which processes can run. Also refer to Microsoft's Documentation about Mandatory Integrity Control.

What is a Restricted SID?

A restricted ID is an access token that modifies a user's access to securable objects and controls a user's ability to perform various system-related operations on the local computer.



When a restricted process or thread tries to access a securable object, the system performs two access checks, using the

- token's enabled SIDs, and
- the list of restricted SIDs.

Access is granted only if both access checks allow the requested access rights.

When to use restricted ID

Use a restricted SID to further restrict the applications in the sandbox, which you can use as another method of monitoring. In other words, this is a way to protect yourself against unknown applications if you don't want to implement a blocking policy.

The restricted SID will allow only Read access to the user registry but not to the local machine registry. Also, restricted processes do not have rights to open any network-based resource, such as file servers. As a result, the restricted SID will be able to do very little and apps may not work correctly under this model. Ultimately, apps in the sandbox that have restricted SID applied to them will be severely locked down.

Using Apply Restricted SID

When you select Restrict Rights and then Apply Restricted SID, you add the Restricted SID to the process. When evaluating security for any operation, when there is any Restricted SID specified then not only does the Security Descriptor need to allow access to the user, but explicitly to the Restricted SID.

How to Add Windows Permissions

Windows permissions are specific OS based permissions to perform actions, like changing system time or taking ownership of a files vs. accessing securable resources. To learn more about these Windows Privileges visit Microsoft's Documentation about User Rights Assignment.

How to Use Well-known Accounts

In this area you will most likely specify either of the following:

- High Mandatory Level
- Low Integrity Level
- Medium Integrity Level
- Medium Plus Integrity Level
- Restricted Code Well Known Group
- System Integrity Level
- Untrusted Mandatory Level

These integrity levels determine who else can use a specific process. Processes launched by a standard user are by default medium integrity. Any process that gets launched via an elevated policy has a high integrity level assigned by default.

Processes need to have level parity to be able to utilize each other. This means, if a process is running at a high integrity level and wants to inject code into another process, it can do so if that other process is running at high, medium, or low integrity levels, but it cannot inject code into system level processes. Processes that run at low integrity levels can be utilized by pretty much any other process, but they cannot reach out to other processes.

New processes are always created with the minimum of the user integrity and file integrity levels. This guarantees that a new process never executes with higher integrity than the executable file.

Example Scenario

In Privilege Manager we can use these Well-known Accounts to set or remove level integrity independent of or in combination with any assigned elevation or blocking policies.

For example, Adobe applications are generally part of elevation policies in an organization. As mentioned before an elevation policy defaults to a high integrity level. Due to Adobe interoperability requirements within their product suites and with processes launched by standard users, it requires medium integrity levels for all Adobe products.

Any elevation policy pertaining to Adobe products, needs an **Adjust Process Rights Action** that sets the **Well-known Accounts** setting to **Medium Integrity Level**.

Additional Options Explained

Under Additional Options customers can select to **Use User's Unrestricted Token** and **Disallow changes to the process rights after applying changes**.

The use of the unrestricted token option is another level of available customization beyond what can be enabled or disabled via the Adjust Process Rights Settings. Enabling this token presents the user with extra levels of access rights over the process. If changes to the process rights are disallowed, the user's unrestricted token is valid as long as the pertaining process is running.

For example if you have a standard user policy for a certain process to run at medium integrity level, but you want to enable more rights without fully elevating and granting the process a high integrity level, you can use the unrestricted access token to fine tune.

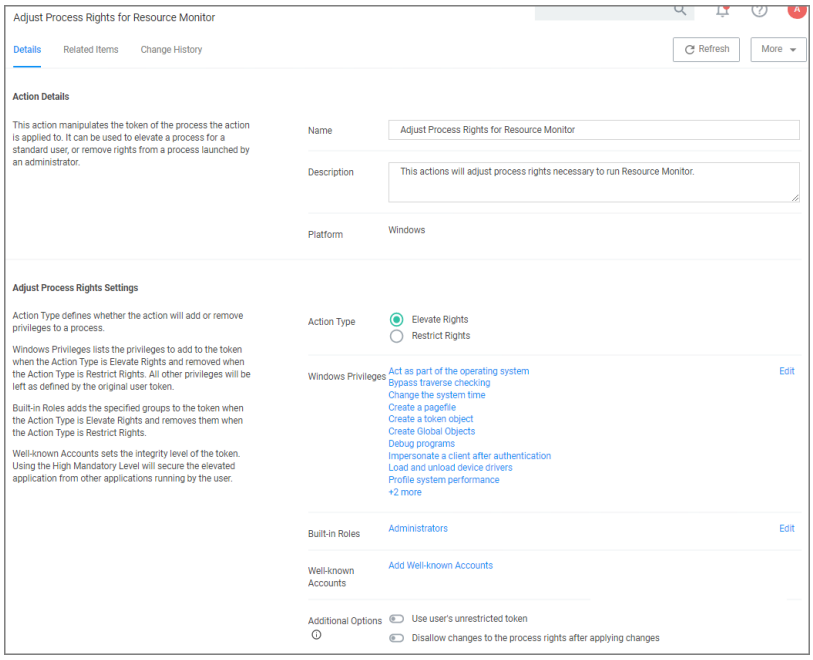
Enabling Unrestricted Token Use

To set the unrestricted token, follow these steps:

1. Select the action of type **Adjust Process Rights Action** that best fits your specific business need.
2. Create a copy of that action.
3. Select the **Use User's Unrestricted Token** checkbox on the copied action and save the action with a new name (for example "Unrestricted Token - Add Admin Rights").
4. Add the new action to new policies or change existing policies and remove the old action.
5. Add the new action and save the changes.
6. Then update the agent client policies.
7. The ACS agent must retrieve the details of the new action from the server via the ACS web service.
8. The change may take a few minutes to reach the client machine after the client policies have updated depending on how busy the server is.

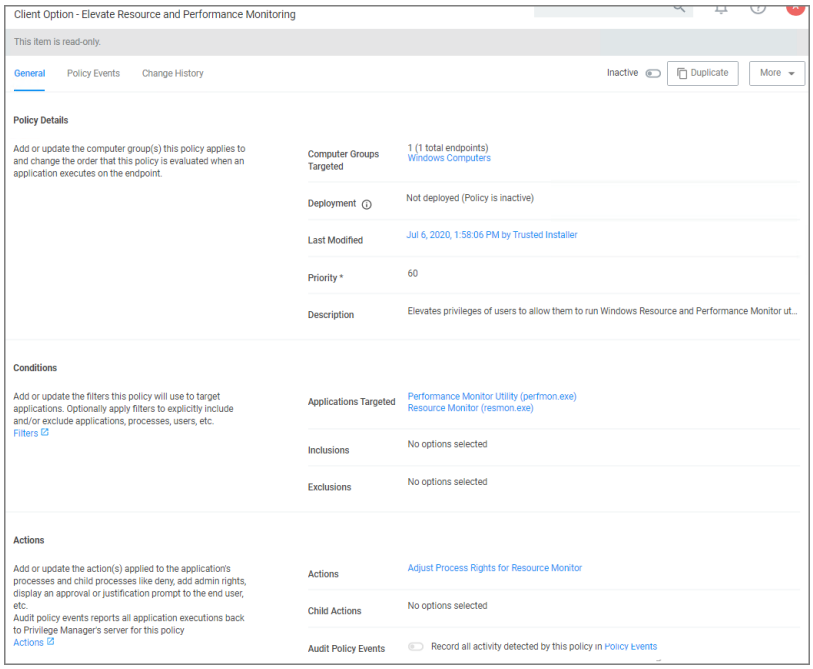
Adjust Process Right for Resource Monitor

The following image shows the default action. To customize make a copy to change any of the default items.



Related Item - Policy

The following image shows the default related item policy for the above action. To customize make a copy to change any of the default items.



Restricting Management for User Accounts and Local Groups

The **Block Local User Management** and **Block Local Group Management** actions prevent specific sets of Win32 API functions from being called. The following functions are blocked from being called:

- NetUserAdd()
- NetUserChangePassword()
- NetUserDel()
- NetUserModalsSet()
- NetUserSetGroups()
- NetUserSetInfo()
- NetLocalGroupAdd()
- NetLocalGroupAddMember()
- NetLocalGroupSetInfo()
- NetLocalGroupDel()
- NetLocalGroupDelMember()
- NetLocalGroupSetMembers()
- NetLocalGroupAddMembers()
- NetLocalGroupDelMembers()

Any process these restrictive actions have been applied to will be unable to call those functions. It makes no difference if the program is .NET (for example, C#) or native code, nor does it make any difference if it is PowerShell (for example, powershell.exe, powershell_ise.exe, pwsh.exe), any of the administrative utilities that are installed along with with Windows (for example,the NET command, mmc.exe) or any third-party supplied application program.

In practical terms, when these actions are applied to both C:\Windows\System32\NET.EXE **and** C:\Windows\System32\NET1.EXE, then the following usages of the NET command (for example, NET command executed from within CMD.EXE or any edition of PowerShell) will be blocked:

- NET USER /ACTIVE:<yes|no>
- NET USER /COMMENT:""
- NET USER /DELETE
- NET USER /ADD
- NET LOCALGROUP /ADD
- NET LOCALGROUP /DEL
- NET LOCALGROUP /COMMENT:""
- NET LOCALGROUP /DELETE
- NET LOCALGROUP /ADD

Likewise, when these actions are applied to any edition of PowerShell, the following cmdlets will be prevented from executing properly:

- Disable-LocalUser
- Enable-LocalUser
- New-LocalUser
- Remove-LocalUser
- Rename-LocalUser
- Set-LocalUser
- Add-LocalGroupMember
- New-LocalGroup
- Remove-LocalGroup
- Remove-LocalGroupMember
- Rename-LocalGroup
- Set-LocalGroup

In .NET, all classes under the `System.DirectoryServices.AccountManagement` namespace that manage user accounts (`UserPrincipal`) and/or local groups (`GroupPrincipal`) are subject to the same restrictions as those classes ultimately make use of the Win32 API functions for which access has been restricted. This is important note as all editions of PowerShell are capable of directly invoking .NET class methods as well as being capable of dynamically compiling & executing C# code, which can then utilize `PInvoke` to make direct calls to functions in any DLL written in any language and compiled withy any development tools.

Finally, C:\Windows\System32\mmc.exe is the host program in which numerous Windows administration tools are executed when their respective snap-in, as identified by a file with a .mmc extension, are loaded into MMC. If these actions are applied to mmc.exe when a specific snap-in is present on the command line, such as compmgmt.msc, (the Computer Management snap-in), then that instance of MMC is also prevented from performing user and local group management operations.

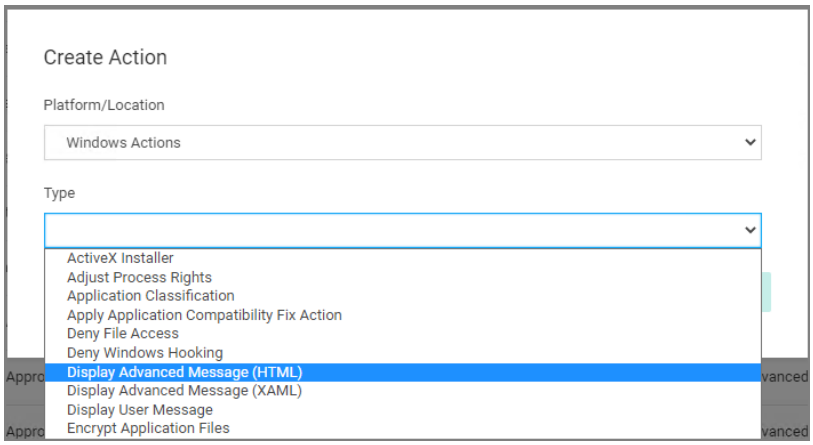
The important thing to remember is that any process that these restrictive actions are applied to will be blocked from making the "forbidden" function calls, regardless of any level of elevation that the process has. Careful attention should be paid to the configuration of policies to ensure that these actions are being applied to elevated processes which are capable of calling arbitrary functions in any available DLL or capable of creating elevated child processes running other programs that are, in turn, capable of make the same types of function calls.

WYSIWYG Display Advanced Message Action Editor

Windows based Display Advanced Message Action types are supported via WYSIWYG editor for user friendly editing of advanced message action text. Any HTML based message can be rendered by the Agent on the Windows endpoint.

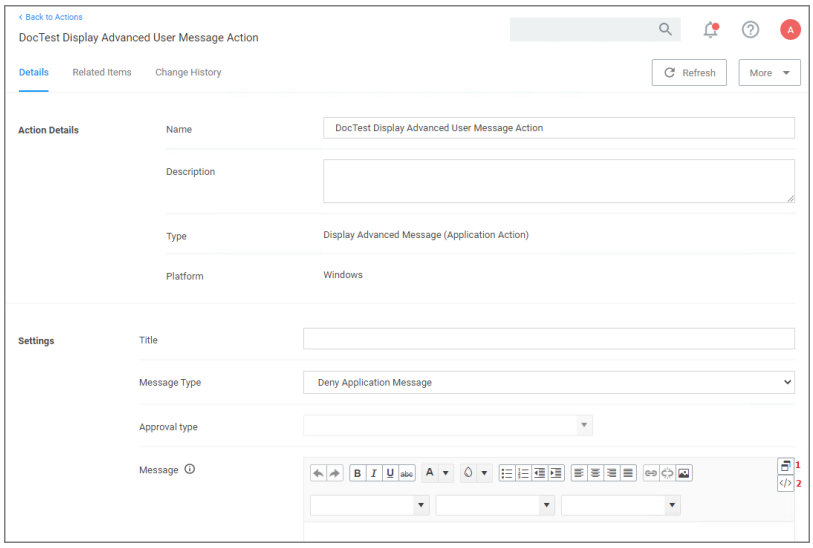
Note: HTML based Advanced Message Actions require an Agent version 11.2.0 or newer.

When you create a new action, for Platform select Windows and from the Type drop-down select Display Advanced Message (HTML).



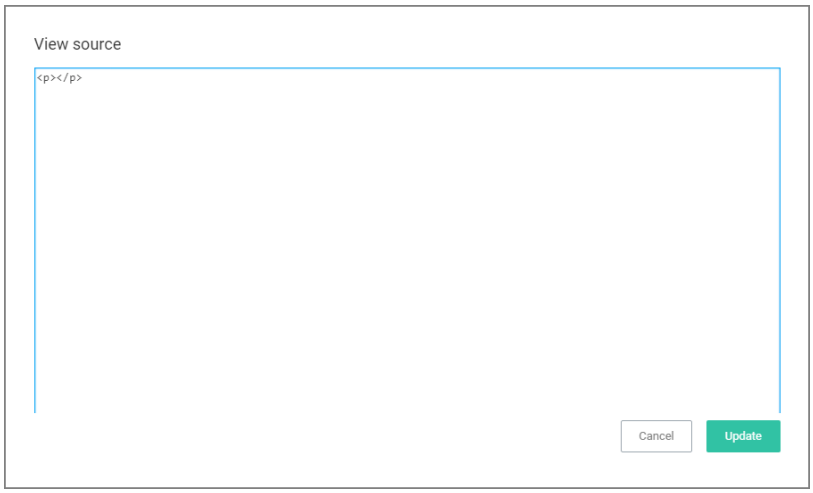
Under Settings, specify the following:

- **Title**, use a message title that indicates what type of action this is for your user on the endpoint.
- **Message Type**, select from the drop-down options:
  - Deny Application Message
  - Warning Message
  - Justification Application Usage
  - Deny Application with Justification
  - Approval Request Message
- **Approval type**, if this is an **Approval Request Message** type action, from the drop-down select if the message is a
  - Default Execute Application Request Type message action, or a
  - Default Offline Execute Application Request Type message action.
- **Message**, use the source view toggle and style/formatting elements to customize your message in HTML.



Where:

- [1] is the undock button, which allows you to edit the page in full-size view.
- [2] is the source toggle, which allows you to enter the HTML source for the message action.



Once you entered the text in the source editor, use the various style element options to format and style your message.

Edit any of the message elements for your users on your endpoints, except for the app-name and user-name variables. Those are system derived.

Any message action should be tested in light and dark mode before populating to endpoints.

Note: You can upload a custom logo, the file size should be under 128 KB and the width should be 500 pixels or less with a maximum hight of 34 pixels.

The logo that is uploaded should NOT be a high-resolution image. Consider that this image will be delivered to every endpoint with every message in which it is used. The smaller the image, the better, for sending the message to the endpoints and for the endpoint to load the message.

Configuration

The Configuration area in Privilege Manager allows users with Privilege Manager Administrator roles to setup new or change existing configurations for areas like user credentials, foreign systems integrations, or authentication. It lets administrators specify settings that control Privilege Manager Server and Console behavior via the Advanced tab.

The Change History tab under Configuration provides users an overview of changes made to configuration items.

When clicking the **?** to the top right, the Configuration page gives the user an overview of the Key Configuration settings and System Health.

The configuration page is tabulated and offers configuration or review options under the following tabs:

- General
- Discovery

- Reputation
- Credentials
- Foreign Systems
- Roles
- Advanced
- Authentication
- Change History

Advanced Tab

The Advanced tab lets you configure settings like:

- General
- API Settings
- Timeout
- Agent
- Inventory
- Monitor
- Proxy
- ServiceBus

To edit any of the advanced settings, make changes and then click **Save Changes**.

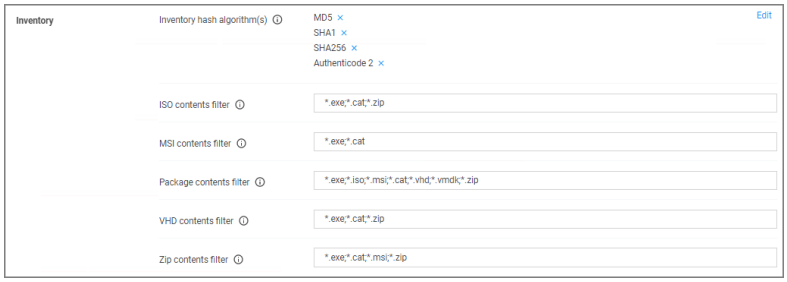
Also refer to Security Algorithms.

File Inventory Solution

Under the File Inventory Solution the inventory hash algorithm(s) and file extensions used for inclusions and exclusions are specified.

- Inventory hash algorithm(s) are the default hash algorithms used for resource inventory. This setting will be used for server-based inventory, and also agent-based inventory unless overridden by agent configuration.
- ISO contents filters with default extensions of .exe, .cat, and .zip.
- MSI contents filters with default extensions of .exe, and .cat.
- Package contents filters with default extensions of .exe, .iso, .msi, .cat, .vhd, .vmdk, and .zip.
- VHD contents filters with default extensions of .exe, .cat, and .zip.

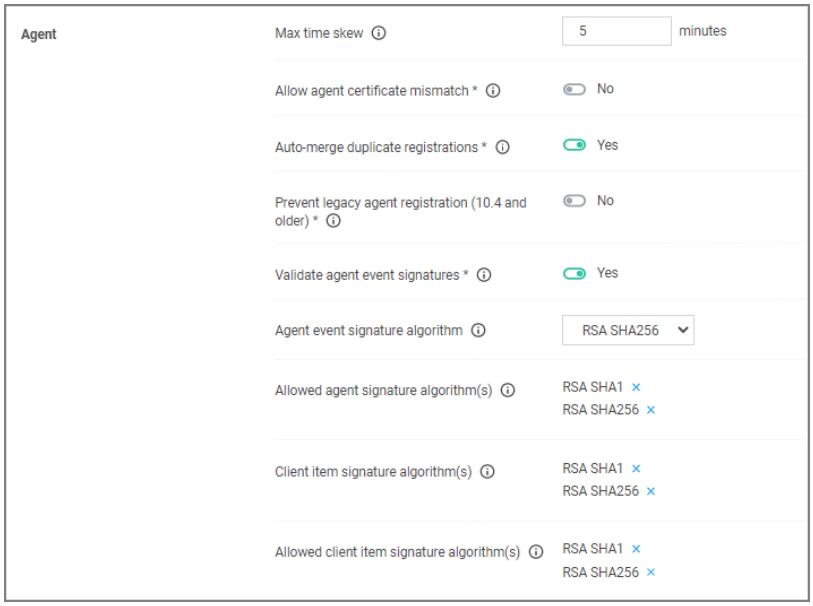
- ZIP contents filters with default extensions of .exe, .cat, . msi, and .zip.



1. To add inventory hash algorithms, click **Edit**. To remove them, click **x**.
2. To change any of the listed file extensions, add or remove extensions directly in the text fields.
3. Make sure to save any changes.

Agent

Under the Agent section the agent related general configuration items can be specified.



Max Time Skew

This setting specifies the maximum time difference (in minutes) to allow client system clocks to be out of sync with the server.

Allow Agent Certificate Mismatch

Enabling this setting, allows agents to communicate with the server even if there is a certificate mismatch.

Auto-Merge Duplicate Registrations

By default this setting is enabled. The setting controls whether or not duplicate SIDs detected during agent registration are automatically merged.

Prevent Legacy Agent Registration (v10.4 and older)

Enabling this setting prevents older agents (prior to v10.5) from registering, allowing only agents with valid agent Install Codes. Only enable this option if you are certain your managed computers have all been upgraded to v10.5 or newer agents.

Validate Agent Event Signatures

By default enabled, this setting will verify the signature contained within agent events are sent to the server. Any events with invalid signatures are discarded.

Agent Event Signature Algorithm

The default signature algorithm agents will use when sending events to the server. Agents 11.1 and newer will use this setting, older agents will use RSA SHA1.

Allowed Agent Signature Algorithm(s)

This setting specifies the algorithm(s) the server should accept for agent event signatures. SHA1 should be left enabled if agents older than 11.1 are in the environment.

Client Item Signature Algorithm

This setting specifies the algorithm(s) used to sign client items that are sent to agents. SHA1 should be left enabled if agents older than 11.1 are in the environment.

Allowed Client Item Signature Algorithm(s)

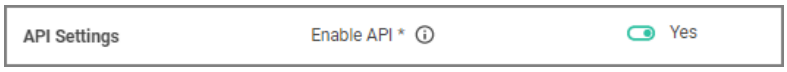
This setting specifies the algorithm(s) the agent should accept for client item signatures. Agents 11.1 and newer will use this setting, older agents will use RSA SHA1.

API Settings

Enable API

Enabling this setting will allow authorized calls to the public facing application programming interface.

1. Set the switch to Yes to enable the API.

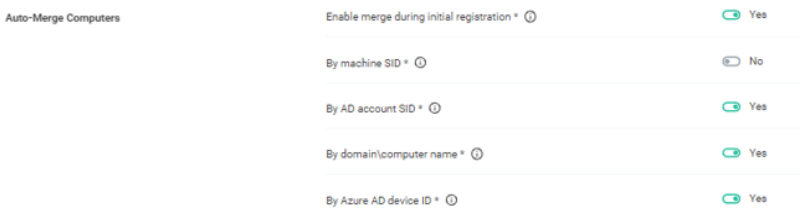


You will need to create an API Client User and assign a role to this user.

Auto-Merge Computers Configuration

The settings here allow users to choose how Computers, Domain Users and Domain Groups with duplicate ID's are dealt with during registration and when the 'Merge Duplicate Resources' task is run.

Note: In order to resolve any issues with duplicate IDs, a user must run these tasks manually.



The **Enable merge during registration** setting will determine whether new computers will be merged into one, if they share attributes with any existing computers associated with the Privilege Manager console.

If this is set to **No**, new computers sharing any attributes will not be merged upon registration, causing a duplicate computer to be created. If it is set to **Yes**, the computer will be merged upon registration, based on the settings below:

By machine SID refers to the Domain SID. If this option is set to **Yes**, and if it is identified that the new computer shares the same Domain SID as any existing computers during computer registration, they will be merged together. If this is set to **No**, new computers with a duplicate Domain SID will be merged upon registration, causing a duplicate computer to be created.

Note: If the **Merge Duplicate Resources** or **Merge Specific Resources** tasks are run, the setting here will be used to determine whether any existing Computers on the system with duplicate Domain SIDs will be merged.

By AD account SID refers to the Account SID. If this option is set to **Yes**, and if it is identified that the new computer shares the same Account SID as any existing computers during computer registration, they will be merged together. If this is set to **No**, new computers with a duplicate Account SIDs will be merged upon registration, causing a duplicate computer to be created.

Note: If the **Merge Duplicate Resources** or **Merge Specific Resources** tasks are run, the setting here will be used to determine whether any existing Computers, Domain Users or Domain Groups on the system with duplicate Account SIDs will be merged.

By domain\computer name refers to the Account Name (e.g., domain\computer). If this option is set to **Yes**, and if it is identified that the new computer shares the same Account Name as any existing computers during computer registration, they will be merged together. If this is set to **No**, new computers with a duplicate Account Name will be merged upon registration, causing a duplicate computer to be created.

Note: If the **Merge Duplicate Resources** or **Merge Specific Resources** tasks are run, the setting here will be used to determine whether any existing Computers, Domain Users or Domain Groups on the system with duplicate Account Names will be merged.

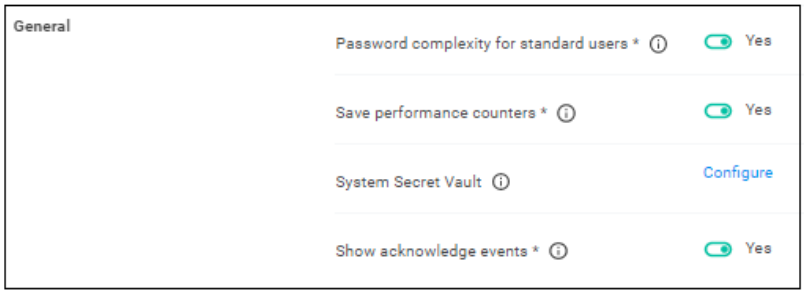
By Azure AD Device Id refers to the Device ID. If this option is set to **Yes**, and if it is identified that the new computer shares the same Device ID as any existing computers during computer registration, they will be merged

together. If this is set to **No**, new computers with a duplicate Device ID will be merged upon registration, causing a duplicate computer to be created.

> **Note:** If the **Merge Duplicate Resources** or **Merge Specific Resources** tasks are run, the setting here will be used to determine whether any existing Computers on the system with duplicate Device IDs will be merged.

General System Settings

Under the Privilege Manager Server category, the first section is **General** settings.



Your client id

This client id is used by **mobile devices** for authentication.

Your tenant id

This tenant id is used by mobile devices for authentication.

Password Complexity for Standard Users

This setting is set to yes by default, meaning the password complexity rules are enforced when creating or editing a Privilege Manager user resource.

Refer to Password Complexity Enforcement for further details.

Save Performance Counters

If this setting is selected, the performance counter data will be recorded in the database. Also refer to Delete Old Performance Counter Events.

System Secret Vault

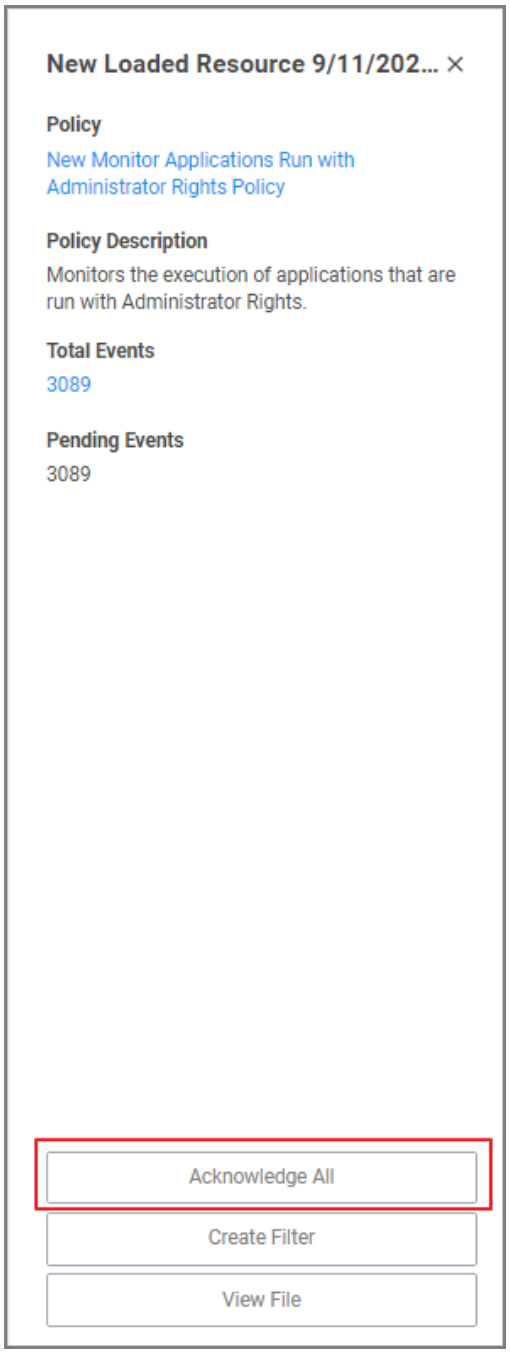
This link lets you configure the foreign system used to store secrets.

Show Acknowledge Events

If selected then the acknowledge events button will be visible in Policy Events.

1. Set the switch to **Yes** to enable the acknowledge events button.

Once you save the changes, you will see **Acknowledge All** on the Policy Events grid after selecting an unacknowledged event.

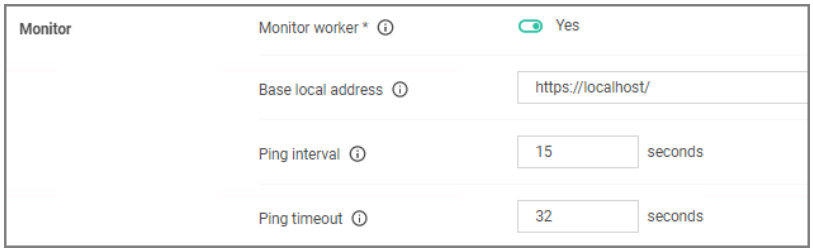


Maximum Application Event Count

This setting specifies the Maximum number of application action events that will be kept in the database. The default setting is 1,000,000. Also refer to Purge Maintenance - Application Control Events.

Monitor Settings

Under the Privilege Manager Server category, the second section is Monitor settings. The Monitor setting is designed to monitor the Worker Role to ensure it is healthy and active. When enabled, the process checks the health at each Ping Interval and waits until the Timeout value before considering it unhealthy.



Monitor Worker

When this setting is enabled the health of the monitor process will be polled.

Base Local Address

This setting specifies the base URL of the Monitor process.

Ping Interval

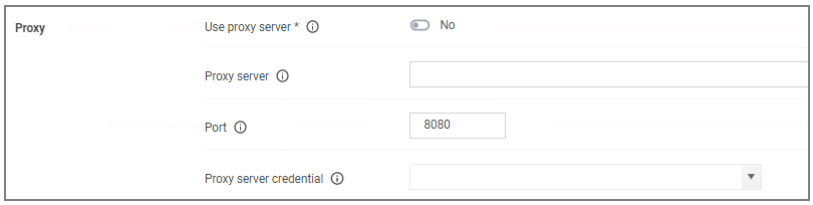
Specifies how often the server will attempt to contact the Monitor process to query its health. The default is set to 15 seconds.

Ping Timeout

Specifies how long the server process will wait to hear back from a ping request to the Monitor process. The default is set to 30 seconds.

Proxy Settings

The proxy configuration settings are used when a reverse proxy is used with your Privilege Manager instance.



Use Proxy Server

If set, communications will be done via the proxy server specified.

Proxy Server

This setting specifies the name or IP address of the proxy server.

Port

This setting specifies the port used for communications to the proxy server.

Proxy Server Credential

This link lets you configure the credential used to authenticate with the proxy server.

ServiceBus

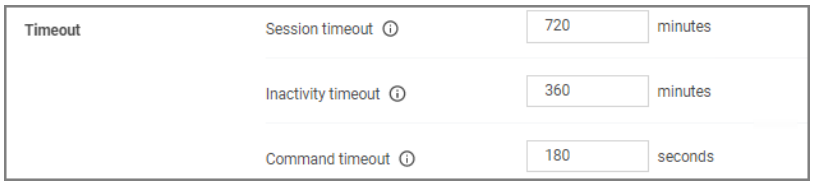
The ServiceBus configuration setting is used when you utilize a Service Bus with your Privilege Manager instance.

Connectivity Mode

This setting specifies the connectivity mode for Service Bus. The default is HTTPS, which is also recommended.

Timeout

These settings specify the system timeout behaviors.

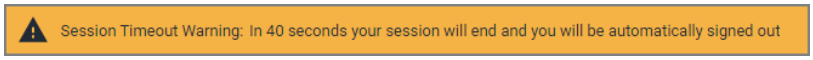


Session Timeout

This setting specifies the maximum time in **minutes** for a login session to be active without having to negotiate another token. The default is set to 720 Minutes (12 Hours).

Session Timeout Warning

Two minutes before the set session timeout window expires, Privilege Manager displays a yellow warning with countdown timer to inform users about the pending session timeout.



Inactivity Timeout

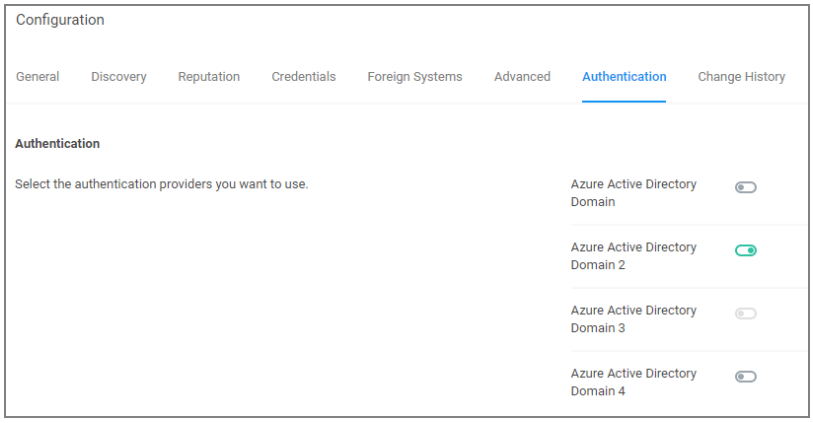
This settings specifies the maximum allowed time for inactivity when logged into the Privilege Manager console. The default is set to 30 Minutes. The session token remains active and does not need to be renegotiated when the inactivity timeout happens within the specified session timeout window.

Command Timeout

This settings specifies the SQL command timeout. The default is 180 Seconds.

Authentication Tab

The Authentication tab is used for enabling the Authentication Providers used with Privilege Manager. Different authentication providers can be enabled based on configured Foreign Systems. The user logs in by selecting from one of these active authentication providers on the login page.



Note: If you are trying to change your Authentication Provider specifically to NTLM, Privilege Manager runs a verification to make sure the local built-in Administrators Group is in the Privilege Manager Administrators Role.

Managing Auth Providers

After you've configured your SAML identity provider, configured users, and added users/groups to Privilege Manager roles, you should be ready to enable SAML as an auth provider.

Enable a SAML Identity Provider

1. Click the slider on the name of your SAML Identity Provider to enable it and save changes.

Note: You can't disable the auth provider used for the current user. To ensure things are setup correctly, you're required to login with a different auth provider before disabling an existing one. You shouldn't rely on a single auth provider, it's best to have a backup in case of any unexpected foreign system issues.

Login

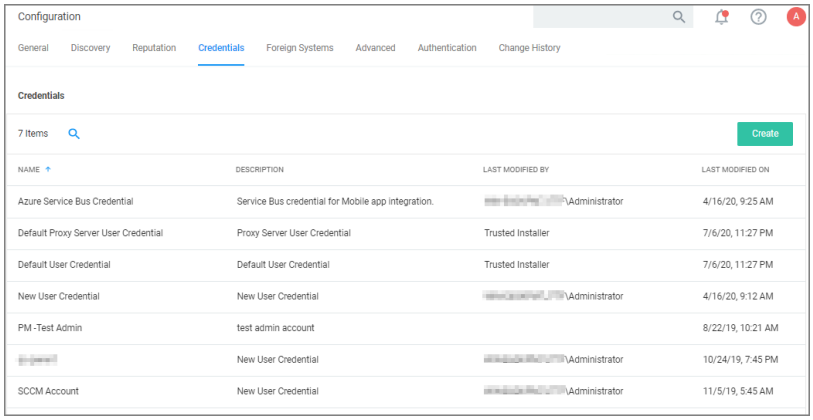
After you've saved auth provider changes, you can logout and test your setup.

1. Click the name of your SAML Identity Provider.
2. You'll be redirected to the configured provider, where you can sign in.

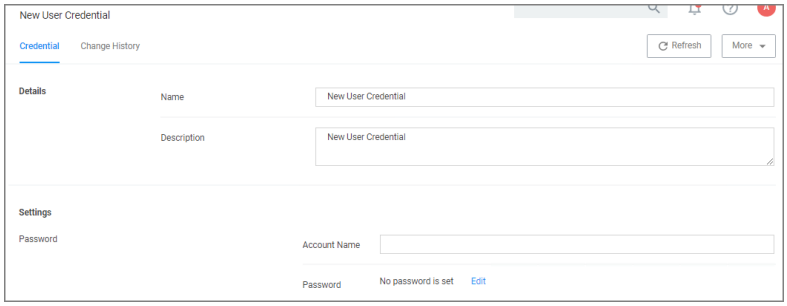
Note: Make sure you're not already signed into the SAML Identity Provider. For example, if your provider is Okta and you've been using the Okta configuration UI, it will try to automatically use that user (and if you are not added to the application, it will fail). It's best to do this in a new Incognito/Private window, and or clear cookies and restart the browser before proceeding.

Credentials Tab

The Credentials tab lets you configure and add new credentials required for configured Foreign Systems.



1. Navigate to **Admin | Configuration** and select the **Credentials** tab.
2. Click **Create** to add a new credential.



User Credentials and Roles

As described for the Roles Tab, Privilege Manager comes with a set of default user roles. Those roles can be edited or new ones can be added to the system.

The role for the Privilege Manager Administrator gives permissions to manage all aspects of the Privilege Manager implementation. As a best practice, it is recommended to set-up roles that limit administrative access to tasks directly related with a users job role.

For integrations withSecret Server keep in mind that Privilege Manger has the ability to use Secret Server as its storage container for credentials. This includes credentials for connecting to integrated systems such as Service Now, as well as credentials for local accounts that are managed by Local Security in Privilege Manager. Customers can choose to integrate with Secret Server only (no Vault setup) or Secret Server and Vault. Either option requires Authentication Data setup for Foreign Systems in Privilege Manager. Refer to the Setting up Integration between Privilege Manager and Secret Server topic.

If you are integrating with Active Directory synchronization please refer to Active Directory Synchronization.

Note: If you synced with Azure AD, and then added that user to the Privilege Manager Administrators Role, that Azure AD user has admin rights only, if Azure AD is used as the auth provider. If users login via Thycotic One, use **Admin | Users** to create a new user and then add that new user to the Privilege Manager Administrators Role, refer to How to Add Thycotic One Users Manually.

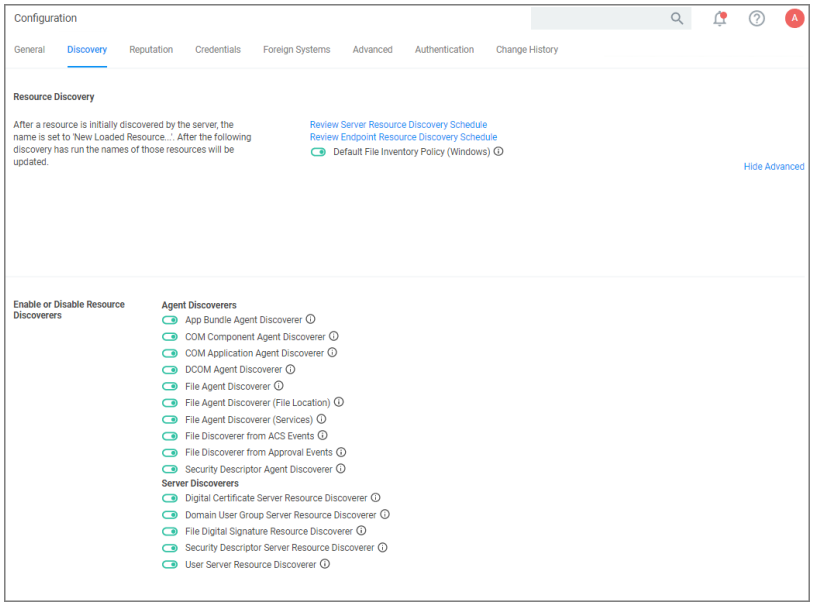
Create User during Installation

During the installation process the Create User page is where you enter information for the initial Privilege Manager Administrator user. Please remember these credentials as they are necessary to login to the web application after you complete the installation.

Discovery Tab

This tab is for resource discovery. After a resource is initially discovered by the server, the name is set to **New Loaded Resource...**. After discovery runs the names of those resources are updated.

Resource Discoverers are selectable under the **Advanced** section. Resource Discoverers are categorized by Agent and Server Discoverers. Most are selected by default and can be disabled via switch.



Refer to Best Practices in the Policy Events section for further details.

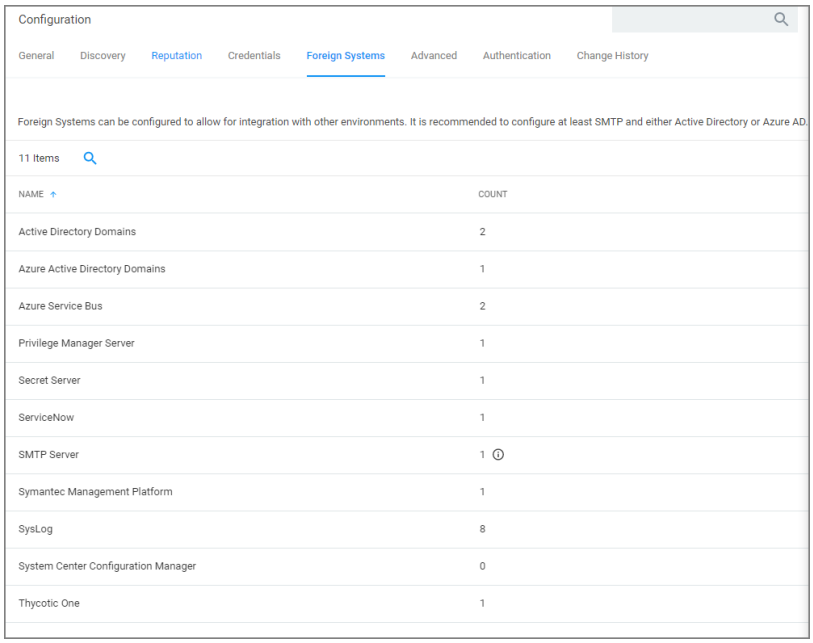
Foreign Systems

Foreign Systems in Privilege Manager are any systems for which a connections or an integration has to be set-up, providing a system URL (network address) and authentication information. Foreign Systems can be Delinea or third-party products and their basic integration set-up in Privilege Manager is alike.

Foreign Systems Tab

Foreign Systems can be configured to allow for integration with other environments. It is recommended to configure at least SMTP and either Active Directory or Azure AD.

In order to use Secret Server as the password vault please review Setting up Integration between Privilege Manager and Secret Server.



Integrations

Delinea Foreign Systems

- Integration between Privilege Manager and Secret Server
- Integration between Privilege Manager and PrivilegedBehaviorAnalytics
- Thycotic One and Privilege Manager Cloud

AD Integration

- Setting Up Azure Active Directory Integration in Privilege Manager

Third-Party Foreign Systems Integration

- Setting up an SMTP Server Connection
- Setting up a Cylance Connection
- Setting up a ServiceNow Ticketing Connection
- ServiceNow Application
  - ServiceNow Application
  - Setting up a ServiceNow Webhook
- Setting up a ServiceNow Webhook Connection
- Setting up VirusTotal

- Setting up an SCCM Connection
- Setting up Syslog

Active Directory Integration

By adding an Active Directory Domain the system can synchronize users, groups, and computers. Once configured a directory synchronization task will need to be started to actually import AD information. Default User Credentials need to be created as well for the system to be able to connect.

The following topics are available in the Active Directory (AD) integration section:

- Setting Up Local Active Directory Synchronization
- Setting Up Azure Active Directory Integration in Privilege Manager - v10.6 and up

Active Directory Synchronization

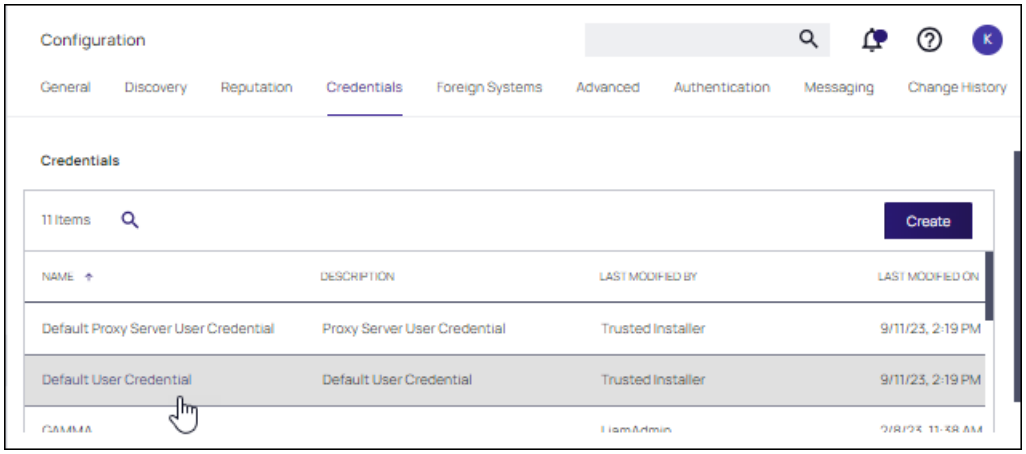
The following procedures show the steps necessary to set-up Active Directory synchronization in Privilege Manager.

If you already configured the AD Default User Credential skip to the Foreign Systems set-up procedure.

Note: For local AD synchronization with Privilege Manager cloud the Directory Services Agent has to be installed. We recommend installing the Directory Services Agent on a system that already has the Delinea Agent (Core Agent) installed; however you may also use a domain connected system and newly install both the Core and Directory Services Agent by using the bundled installer.

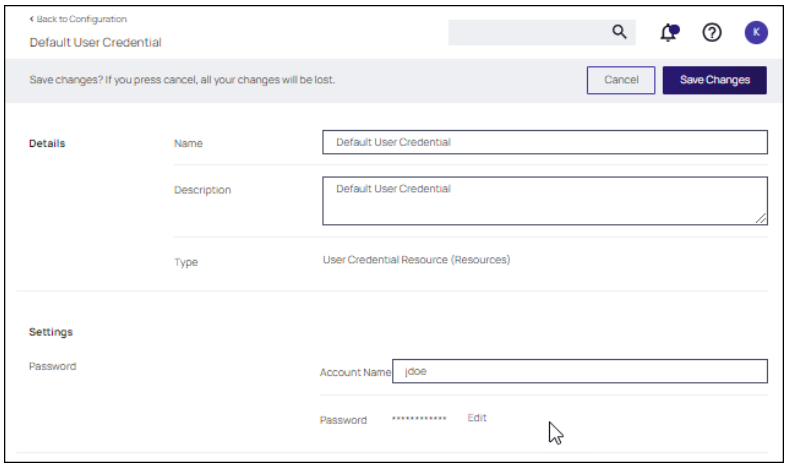
Set Up AD Default User Credential

1. Select **Admin | Configuration**.
2. Select the **Credentials** tab.
3. Edit the **Default User Credential** or use **Create** to add a new user.



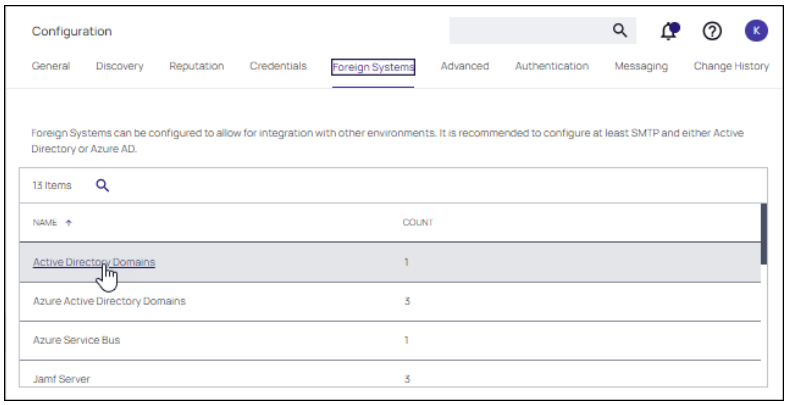
4. Set a domain credential with an Account Name and Password that can read from the Active Directory domain

(s).Click **Save Changes** and continue with step 2 in the Foreign Systems set-up procedure.



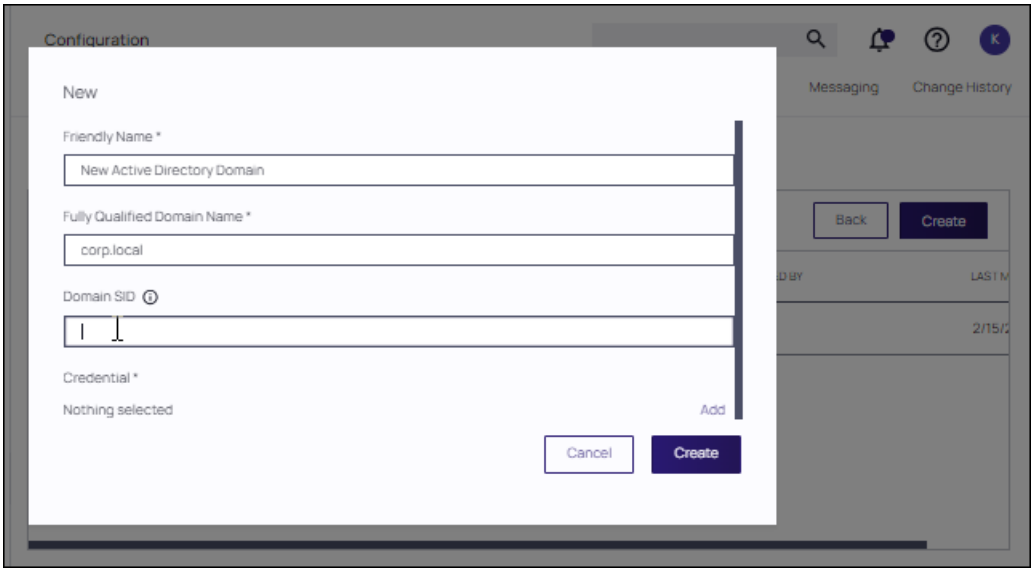
Set Up Foreign Systems

1. Select **Admin | Configuration**.
2. Select the **Foreign Systems** tab.
3. Select **Active Directory Domains**.



4. On the Active Directory Domains page, select **Create**.

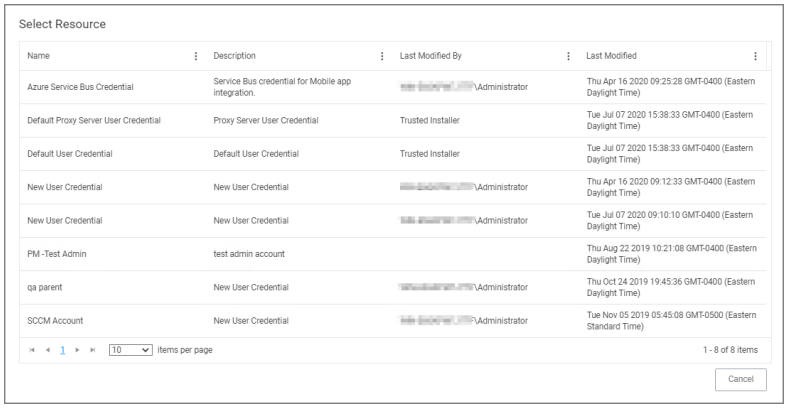
a. Enter a fully qualified domain name and a friendly name.



b. Enter a SID. To find your SID, open a PowerShell window and type: `Get-ADDomain`. Your SID appears in the **DomainSID** field.

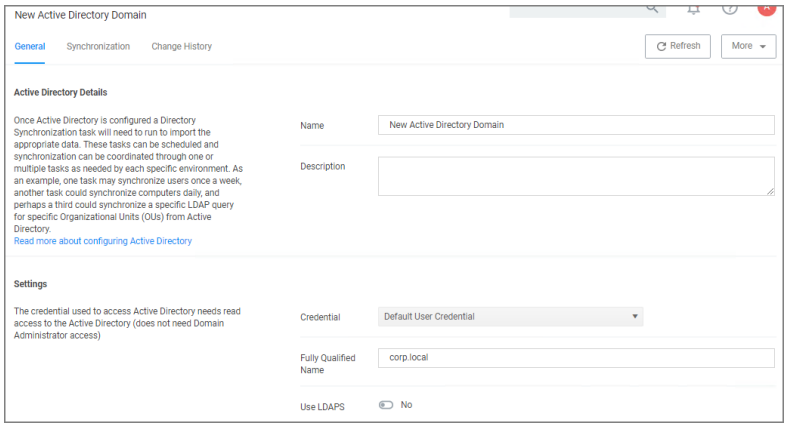
> **Note:** An SID is required.

5. Under the required Credential click **Select...**.

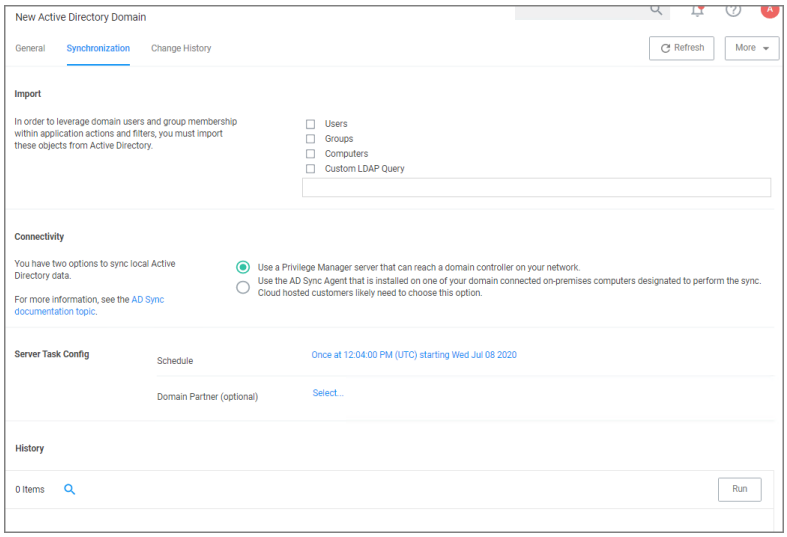


6. From the Resources page select a credential.

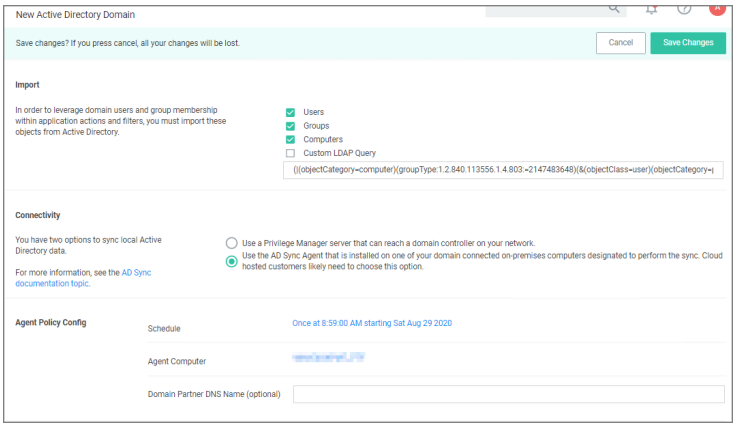
7. Click **Create**.



8. Verify the **URL** (Fully Qualified Name) is correct.
9. If the domain uses LDAPS, set the switch to enable.
10. Click **Save Changes**.
11. Once Active Directory is configured a Directory Synchronization task needs to run to import the appropriate data. Select the **Synchronization** tab.



12. Select the task(s) you want to perform:
    a. Import:
        - Users
        - Groups
        - Computers
        - Custom LDAP Query
    b. Connectivity, via either
        - **Privilege Manager server** that can reach a domain controller on your network:
            i. Synchronization Task Config:
                - Schedule - Schedules help keeping your system in sync with your domain updates.
                - Domain Partner (optional)
            ii. Click **Save Changes**.
            iii. Click **Run**, to manually run the task on demand.
        - Directory Services Agent that is installed on one of your domain connected on-premises computers designated to perform the sync. Cloud hosted customers likely need to choose this option.

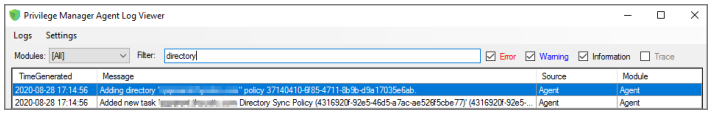


i. Under **Agent Policy Config**:

- Schedule: Schedules help keeping your system in sync with your domain updates.
- Agent Computer: Select the computer that has the Delinea Core and Directory Services Agents installed.
- Domain Partner (optional)

ii. Click **Save Changes**.

By setting this up via Directory Services Agent, the directory policy and the Directory Sync Policy task are applied to the agent, which based on the task schedule kicks off the local active directory synchronization. You can verify this by checking your Agent logs.



Tasks can be scheduled and synchronization can be coordinated through one or multiple tasks as needed by each specific environment. As an example, one task may synchronize users once a week, another task could synchronize computers daily, and perhaps a third could synchronize a specific LDAP query for a specific group from Active Directory.

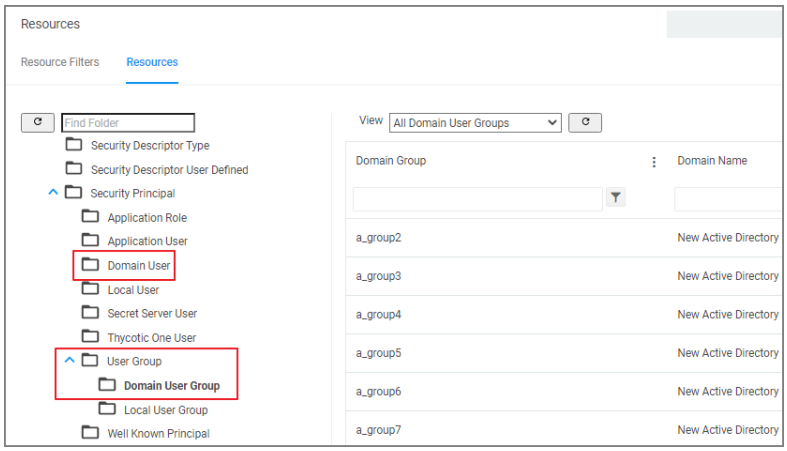
Viewing Imported Users and Groups

You may verify and browse the users and groups that are expected to be imported from Active Directory.

1. In Privilege Manager, navigate to **Admin | Resources**.
2. Expand **Organizational Views**.
3. Expand **Default**.
4. Expand **All Resources**.
5. Expand **Security Principal**.

a. Select **Domain User**. You should see a list that contains imported Active Directory users.

b. Select **User Group**. You should see a list that contains imported Active Directory groups (other groups may exist in the list as well).



Setting Up Azure Active Directory Integration

Note: If replacing an existing Azure Integration, ensure a new integration object is created (don't edit an old one). Delinea recommends recycling your Application Pools.

Setting up Azure AD integration with Privilege Manager requires steps in your Azure tenant and in Privilege Manager.

In Privilege Manager the Azure Active Directory Domain Foreign System requires the following from the Azure Portal:

- Tenant (this is the unique identifier of the Azure Active Directory instance)
- Application ID (an application registration in the directory instance)
- Client Secret (this is found in Certificates & Secrets in the Azure portal for the previously created application registration)

This documentation assumes that you are familiar with the Azure Portal and know how to navigate it in order to setup or retrieve the above information for configuration with your Privilege Manager instance.

Setting up Azure AD Integration in Privilege Manager requires these components independent of On-premises or Cloud:

- User Credential
- An Azure Active Directory Domain Foreign System
- Executing a Privilege Manager Task (Import Users and Groups)
- Creating a Scheduled Task to synchronize the users and groups on a regular basis

Note: You do not need to have an active directory domain before you can sync with an Azure Active Directory. However, there are benefits for synchronizing on-premises Active Directory to Azure AD.

Prerequisites

Assign Azure user(s) to the **Privilege Manager Administrators** Role. In order for users to authenticate via Azure AD, they need to be members of various roles. There must be at least one member from your Azure Directory to be allowed to login via Azure AD before you can continue. We recommend adding yourself to ensure that you can login after the Authentication Provider is configured.

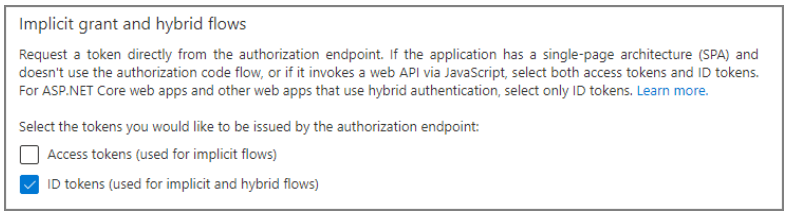
Setting up Azure AD with Privilege Manager

Steps in the Azure Portal

1. Navigate to your Azure Portal: https://portal.azure.com
2. In your Azure portal, navigate to and open **Azure Active Directory**.
3. Verify you are in the right tenant or use **Switch Tenant** to switch to another tenant in your organization.
4. Under **Create** select **App registration**.
5. Under **Register an application**, enter
   a. an application **Name**.
   b. select **Supported account types** based on your business requirements.
   c. specify the following Redirect URI values using the URI of your Privilege Manager server: https://myserver.example.com/TMS/

      Note: This URI does not need to be a publicly visible address. It is only used in redirecting the browser back to the Privilege Manager web application after authentication. For Privilege Manager Cloud subscriptions, the URI should be pointed to the URI that was set up for you, for example: `https://myassignedname.privilegemanagercloud.com/Tms/`

   d. Click the **Register** button.
6. Navigate to your newly created application registration.
7. Enter these additional URIs in the Redirect URI field:
   - `https://myserver.example.com/Tms/Account/Signout/`
   - `https://myserver.example.com/Tms/Account/SignoutCallback/`
8. On the **Platform configurations** page under the **Implicit grant and hybrid flows** area, check the box labeled **ID tokens**.



9. Under **Manage**, select **API Permissions**.
10. Click the **+ Add a permission** option to add the Microsoft Graph API.

11. As permission type, select **Application permissions**.
12. Expand **Directory**, select **Directory.Read.All** and click **Add permissions**.

    Note: If you have upgraded from a previous version of Privilege Manager (and all servers that are using this Azure integration are now at version 11.2.1 or newer), you may remove any previously added Azure Active Directory Graph API rights. This is no longer needed.

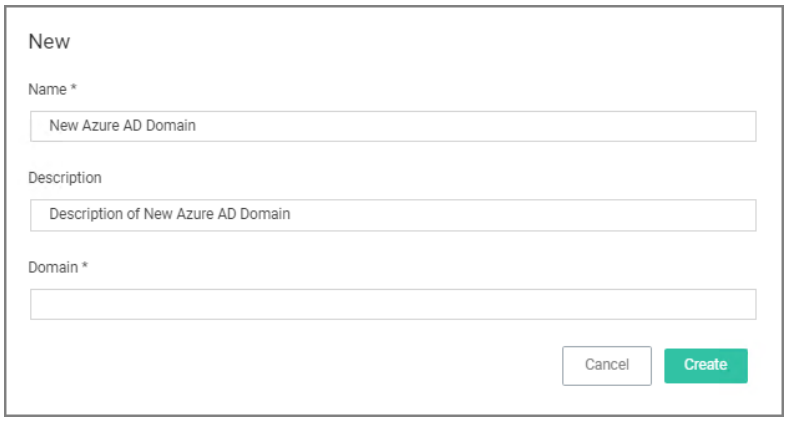
13. Under **Manage**, select **Certificates & secrets**.
14. Click **+ New client secret**.
15. Add a **Description** and choose an **Expires** setting based on your business requirements.
16. Click **Add** to create the secret.
17. Use the **Copy to clipboard** icon to copy the newly created secret to the clipboard.

You will need the Application Id and the Client Secret you copied to the clipboard in Privilege Manager to complete the setup.

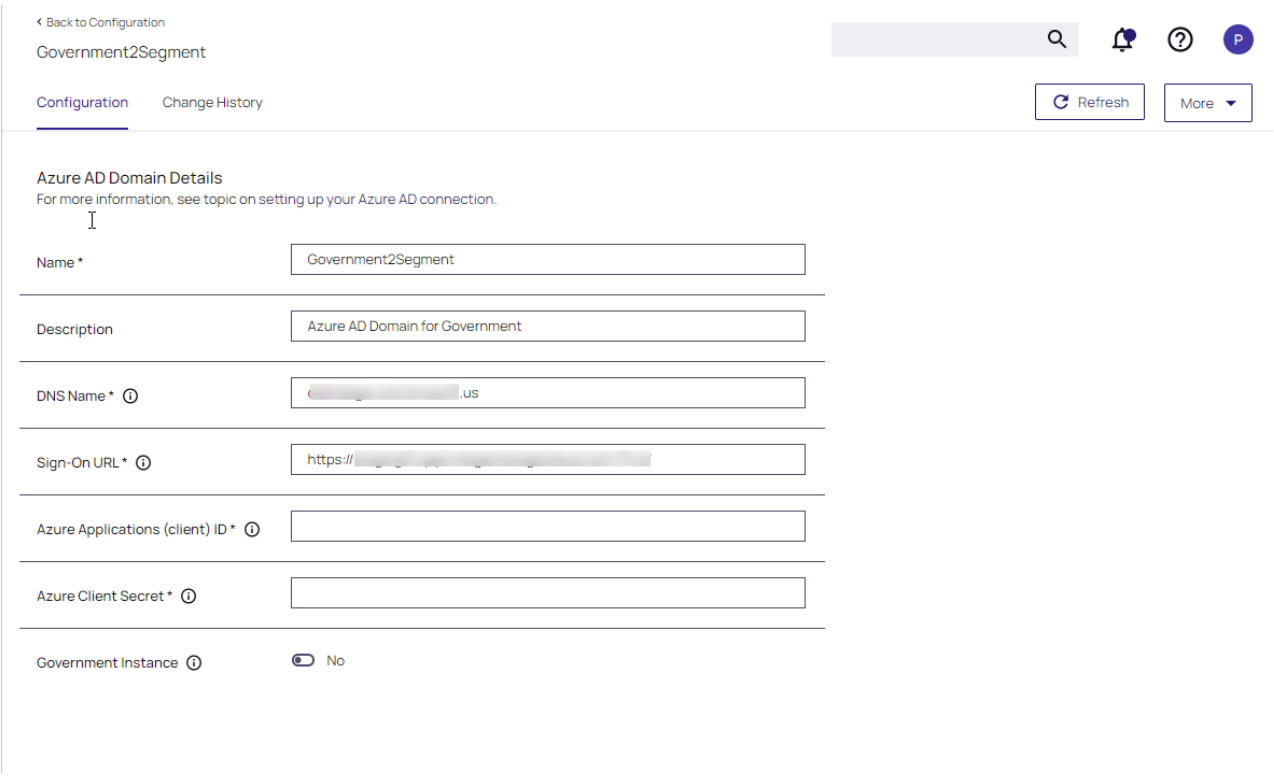
Steps in your Privilege Manager Instance

Set-up Foreign Systems

1. Select **Admin | Configuration**.
2. Select the **Foreign Systems** tab.
3. Select **Azure Active Directory Domains**.
4. Click **Create**.



5. Enter a Name, Description, and Domain, which is the DNS name of the Tenant from the Azure Portal identified at the beginning of this document.
6. Click the **Create**.



7. Verify the **Sign-on URL** is correct. This value should match what was specified in the Redirect URI option when setting up the Application Registration.
8. Enter the **Azure Application (client) ID**. This is the Application ID that was created when registering your application in the Azure Portal.
9. Enter the value of the secret from the Azure Portal into the **Azure Client Secret** field.
10. If the portal will be hosted in the US Government cloud, enable the **Government Instance** toggle.
11. Click **Save Changes**.
12. Continue to the Azure AD Authentication Provider section and click **Edit**.
13. Complete the three steps:
    a. Import Users & Groups from Azure AD. This process may take a few minutes to complete, depending on the size of the directory. Privilege Manager offers various different tasks for this import:
        - **Import Azure AD Resources**, imports ALL users and groups.
        - **Import Directory Computers**.
        - **Import Directory Sites**.
        - **Import Directory Users and Groups**.
        - **Import Directory OU**.
        - **Import Specific Azure AD Users and Groups**, imports only the specified users and/or groups.

Refer to setup and scheduling of these tasks under the "Import Users and Groups via Privilege Manager Task" and "Create Scheduled Task for Users/Groups Synchronization" topics below.

Also refer to the Server Tasks | Foreign Systems | Directory Services for details on the Directory Services tasks.

b. Assign Azure user(s) to the Privilege Manager Administrators Role. In order for users to authenticate via Azure AD, they will need to be added as members of various roles. There must be at least one member from this Azure Directory allowed to login via Azure AD before you can continue. We recommend adding yourself to ensure that you can login after the Authentication Provider is configured.

c. Set as Authentication Provider.

14. Click **Save Changes**.

Viewing Imported Users and Groups

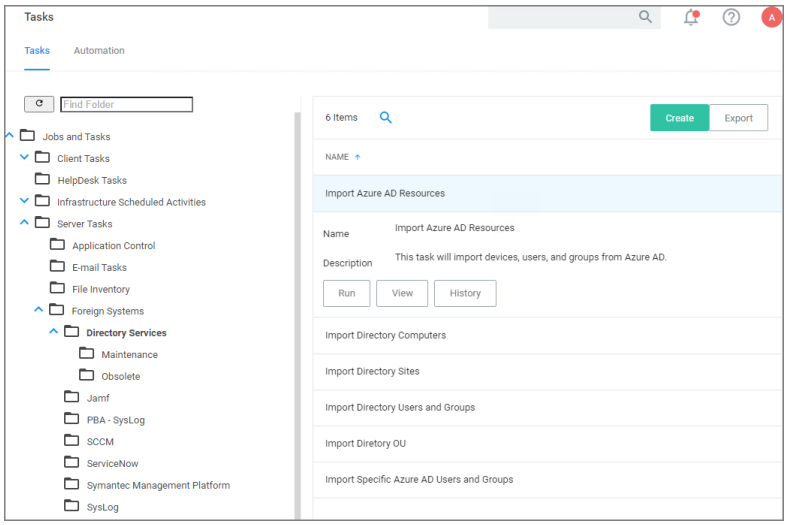
You may verify and browse the users and groups that are expected to be imported from Azure Active Directory.

1. In Privilege Manager, navigate to **Admin | Resources**.
2. Expand **Organizational Views**.
3. Expand **Default**.
4. Expand **All Resources**.
5. Expand **Security Principal**.
6. Select **Domain Users**. You should see a list that contains imported Azure AD users.
7. Select **User Group**. You should see a list that contains imported Azure AD groups (other groups may exist in the list as well).

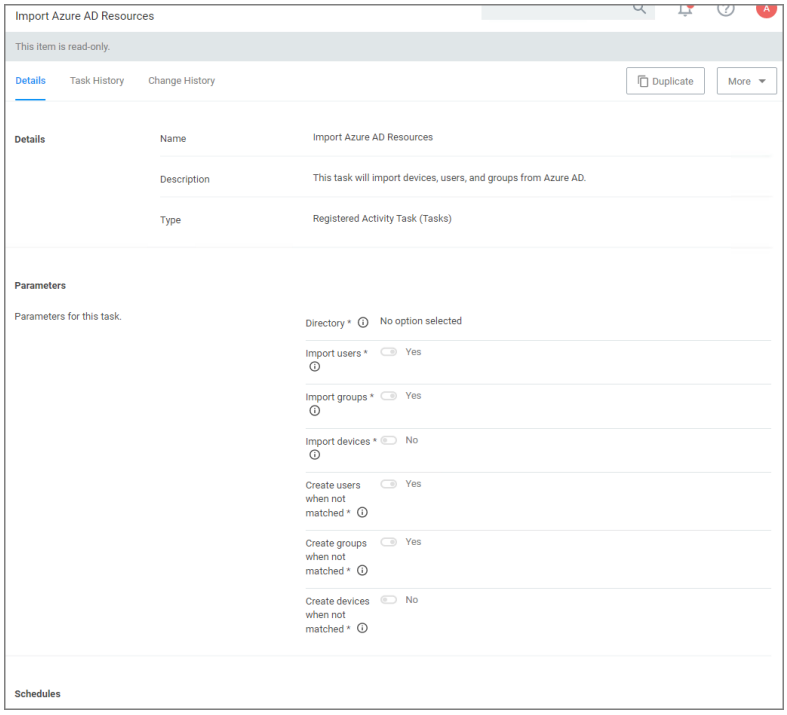
Import Users and Groups via Privilege Manager Task

This step was performed initially as part of setting up the Azure AD directory. To re-import users and groups, you can perform that operation again to pick up changes that may have occurred in the directory, such as new users that have been added or group membership changes. To run this manually:

1. Navigate to **Privilege Manager | Admin | Tasks**.
2. Expand **Jobs and Tasks**.
3. Expand **Server Tasks**.
4. Select **Directory Services**.



5. Click on **Import Azure AD Resources** to import devices, groups, and/or users based on a selected resource.
6. Click **Run**, then **Select Resource** and select from the available resources.



7. Select the Azure Active Directory Domain you previously created.
   a. Enable **Import Devices**.
   b. Enable **Import Groups**.
   c. Enable **Import Users**.
8. Click **Run Task**.

If you only want a subset of the directory to be imported, enable select and enable only the resources you wish to import at this point.

Create Scheduled Task for Users/Groups Synchronization

To schedule this operation to happen on a regular schedule:

1. Navigate to **Privilege Manager | Admin | Tasks**.
2. Expand **Jobs and Tasks**.
3. Expand **Server Tasks**.
4. Select **Directory Services**.
5. Click on **Import Azure AD Resources** to import devices, groups, and/or users based on a selected resource.
6. Click **View**.
7. In the Schedules tab, click **New Schedule** to create a new schedule.
   a. On the **Schedule** tab, define the desired schedule.
   b. On the **Parameters** tab, select the **Azure Active Directory** resource that you created earlier and make selections for importing devices, users, and groups.
8. Click **Save Changes**.

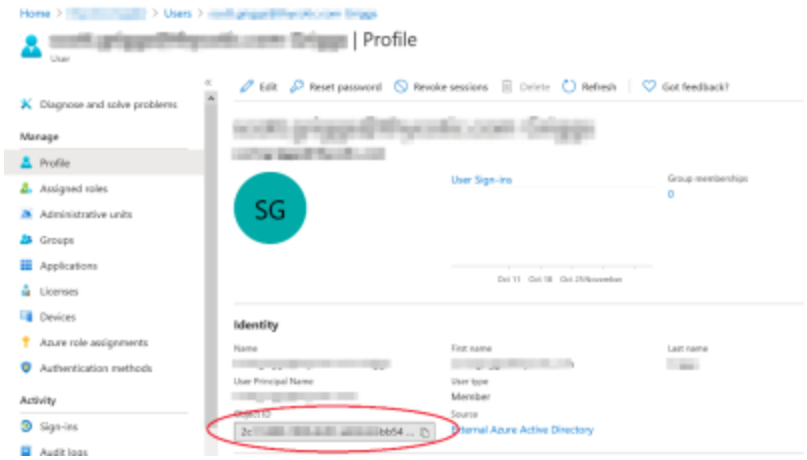
Best Practice: Troubleshooting AD Sync

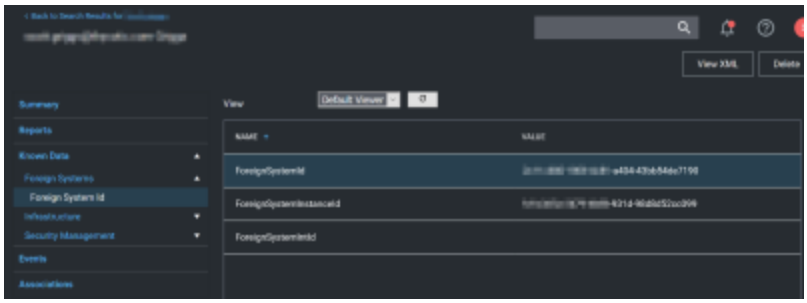
Authentication

Note: Delinea recommends that customers create a new user in Azure AD (one that is not sync-ed from AD) as a Privilege Manager Global Administrator. This user can be used as a backup access if other users fail to sync correctly.

When a user logs in to Privilege Manager with Azure AD, privilege-manager gets back an object ID. A search of the database for that object ID in **ForeignSystemId**, provides what roles that user is a member of. The internal caching uses SID, so the user must also have a Global Account Details - **SID**. If there are any issues with the user authentication, it is recommended to check this data to make sure it exists, and make sure it matches the Azure portal data.

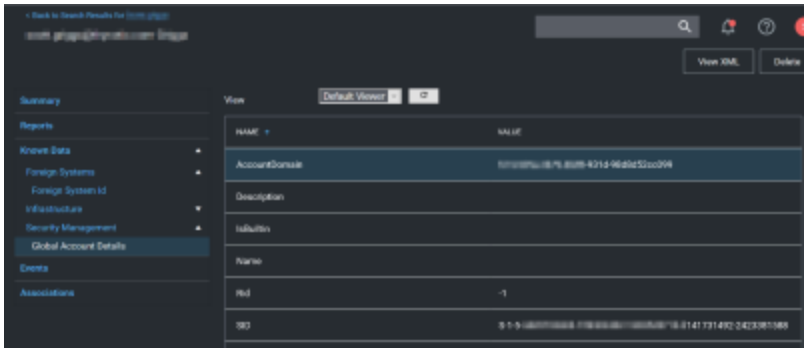
The object ID in the Azure portal should match **ForeignSystemId** in Privilege Manager.





Note: There may be multiple foreign systems entries here, when it doubt browse the Azure AD foreign system, not the GUID in the browser URL, and match that up in the list along with the object ID.

Users also need to have a **Global Account Details - SID** from the same Azure AD foreign system ID.



Note: There may be multiple entries here. If Privilege Manager doesn't have one where the **AccountDomain** matches the foreign system ID, that could potentially point to a problem.

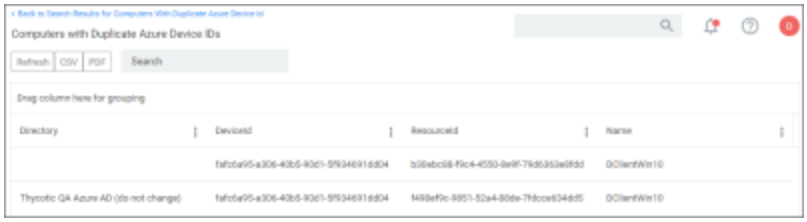
Duplicates

The basic reason for duplicates is not having matching information when Privilege Manager imports resources, registers computers, or updates inventory.

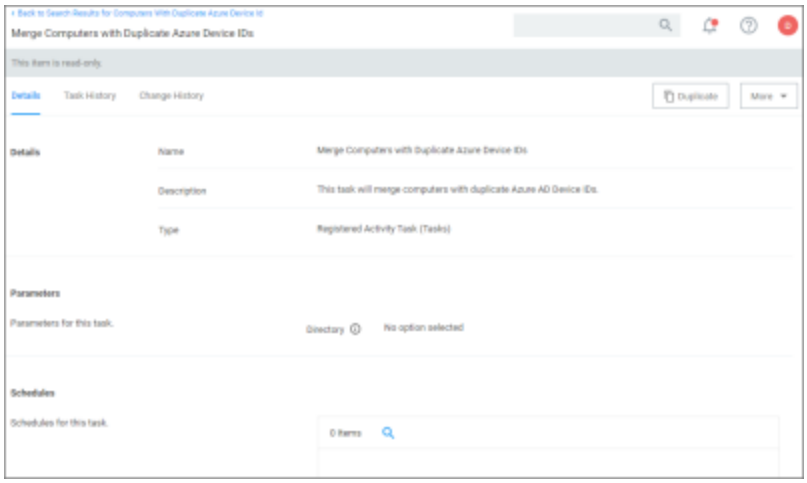
Agent Registration

Prior Privilege Manager version 11.1.0, if you imported devices from Azure AD and then registered agents, you were guaranteed to get duplicate computers. With version 11.1.0, when agents register, the server checks for existing computers with the same **DeviceId** and merges them automatically.

For existing systems where duplicate computers have been recorded, the **Computers with Duplicate Azure Device IDs** report is available.



Run the report and then use the **Merge Computers with Duplicate Azure Device IDs** task to merge all computers with duplicate **DeviceIds** based on the report.



The report and task require a version 11.1.x based agent.

Resource Type Keys

Privilege Manager identifies resources in several ways. The primary way is through “keys," which is basically just uniquely identifying data about a resource. Not all keys are available from all sources, so below each key is a table that lists availability.

Global Account Details - SID

This key is used to match computers, users, and groups based on the SID from their primary domain.

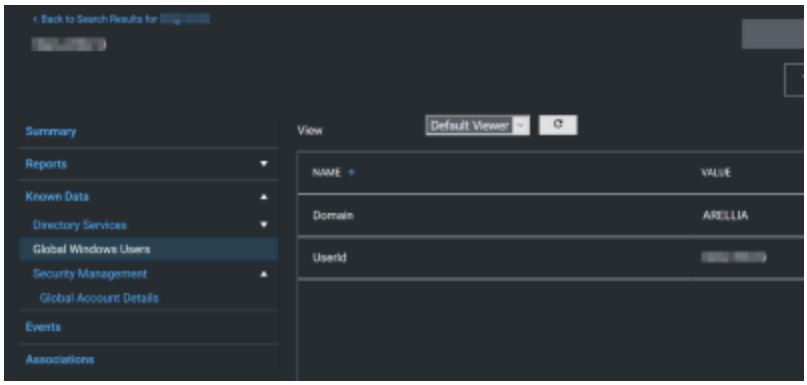
Availability

	Azure AD	AD	Local Inventory	Agent Reg
	Azure AD	AD	Local Inventory	Agent Reg
Users	Yes and No [^1]	Yes	Yes [^2]	N/A
Groups	Yes and No [^1]	Yes	Yes [^3]	N/A
Computers	No	Yes	N/A	Yes [^4]

- [^1] Users and groups created natively in Azure AD will not have a SID.
- [^2] SID may not be available on all Azure AD systems. Users and Groups imported from AD will have a SID (by default, customers can change the settings in Azure AD Connect, so it's typical, but not a guarantee). Devices (computers) in Azure AD will typically not have this information.
- [^3] Starting with the 10.8 agent, when reporting AD domain users and groups that are members of a local group, the agent will include Global Account Details SID. But with older agents it's not reported, and this can be a likely source of duplicates.
- [^4] Starting with the 10.8 agent, when registering the agent will report its SID from the domain to which it's currently connected. Agents that are offline will cache this information for a period of time, but agents long disconnected from the domain will not be able to report this.

Global Windows Users - User Id & Domain Name

This is the key that has the longest history of use in Privilege Manager.



Availability

	Azure AD	AD	Local Inventory	Agent Reg
	Azure AD	AD	Local Inventory	Agent Reg
Users	No [^1]	Yes	Yes	N/A
Groups	No [^1]	Yes	Yes	N/A
Computers	No	Yes	N/A	Yes

[^1] Azure AD can be configured (Azure AD Connect) to report this information for users and groups, but we don't read it when importing. This is planned as a future product update.

Note: Until recently, the agent didn't report SID for domain users and groups. So the agent would report users with name/domain, import from Azure AD would report SID, since there wasn't common data, this was a common source of duplication.

There are a couple of solutions to duplicates here:

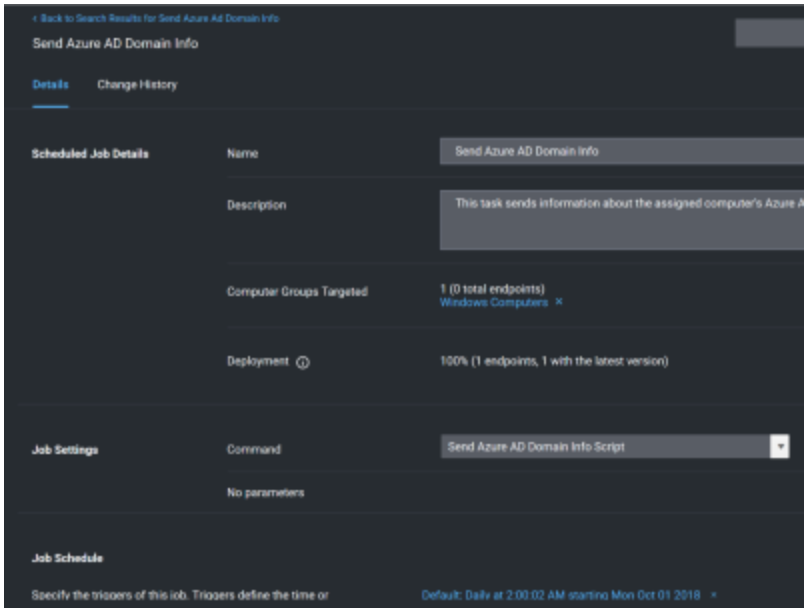
1. Also run an import from AD (typically on-premises AD agent), and then run the task **Merge Duplicate Account SID Resources**. Note that this will not work for computers we can't get SID for computers from Azure AD.
2. Delete the duplicates. When you delete duplicates, delete the resource that is not an agent, and with the least information.

Azure AD - Device ID

This data was added in an attempt to support importing devices from Azure AD. The agent will report Azure AD domain join info which includes Device ID and Tenant ID, and when importing from Azure AD Privilege Manager will attempt to match existing computers before creating a new one.

Send Azure AD Domain Info

This is the agent-scheduled task that reports the Azure AD info, by default it runs at 2 AM daily.

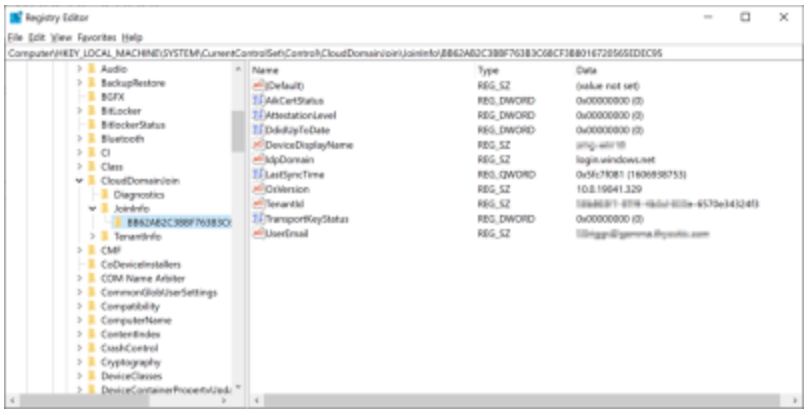


Limitations

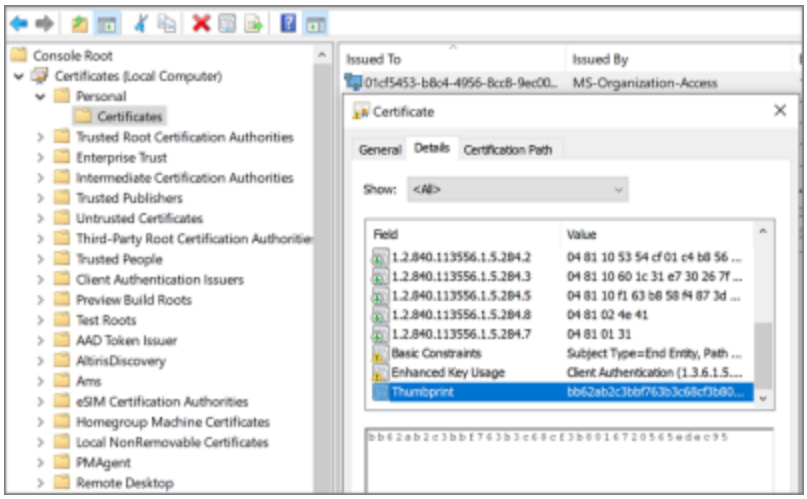
Unfortunately this data is limited to a very specific domain join. Hybrid domain joins (both AD and Azure AD) don't seem to support this. When using hybrid join, all the data seems to be per-user, and currently the agent task to report info only works if the data is global.

Registry/Certificates

If you want to troubleshoot why an agent isn't reporting this domain join info, you can follow in the registry to check the data for yourself. Go to `HKLM\System\CurrentControlSet\Control\CloudDomainJoin\JoinInfo\`. The keys there are named by the hash of the relevant certificate (the image below is for a local user (the one that doesn't work), but the concept is the same).



In this case **6A901B....** is referencing a certificate. The certificate will be in the local machine, personal store (again, the image below is actually for a user's cert, but the concept is the same).



So we find the certificate with thumbprint **6A901B....** and it's subject, in this case **58b863f1-87f4-4b3d-833e-6570e34324f3** is what will be reported, and what we can match up to the Device ID in Azure.

Best Practice: Active Directory Import

On-Prem

The support for on-prem AD import is better than the support for Azure AD. On-prem AD import has more usable data. For customers that want to target computers based on OU or Security Groups, this is the best option. Our customers can setup an AD foreign system with credentials and import directly using LDAP.

Cloud

In a cloud environment the Privilege Manager server(s) typically don't have direct access to Active Directory. Instead, the customer can select a local machine on which to install the Directory Services Agent. The agent retrieves information and sends data to the server on a schedule.

Full vs Differential Synchronization

Unless otherwise specified, both the server and agent imports attempt a differential synchronization of AD data. AD keeps an Update Sequence Number (USN) that goes up as changes are made and resources are added. The following 3 conditions must be met for a differential sync:

1. Privilege Manager has a record of a prior sync with a session ID and USN.
   - On the server these are recorded in the database as data for the foreign system in the [Ams.Data].[DirectorySync] table.
   - For the agent they're recorded in the registry under `HKLM\\Software\\Arellia\\Agent\\DirectoryServices\\Imports`. Users can force a full sync by deleting this data.
2. The directory partner (Domain Controller Server) must be the same. Starting with Privilege Managerversion 10.8 and later, a server will be automatically picked if none is specified. But on older versions of the product, no differential sync is available unless the server is specified.
3. The LDAP query must be the same query as the hash is stored.

Assuming the conditions are met, Privilege Manager takes the given LDAP query, and appends a condition that the USN is greater than the recorded last USN.

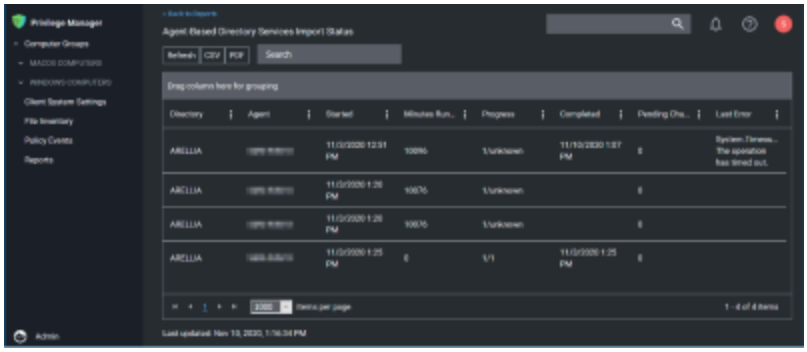
> **Note:** In test environments it's common to have a sync “fail” because the agent has done a sync prior on a different PM server. For a new environment setup with a Directory Services Agent, remember to clear out the registry record of syncs.

Expected Performance

If connectivity is good (low latency is just as important as high throughput), the main bottleneck is writing item data to the Privilege Manager database. Small ADs with a few hundred resources complete in a couple minutes. Large ADs with hundreds of thousands may take 10 hours or more.

Status

For imports run via the Directory Services Agent, Privilege Manager contains a report to give basic status named **Agent-Based Directory Services Import Status**.



When Privilege Manager runs an LDAP query, the number of results returned or how long the process will take is an unknown. The agent reports the data as it gets it in chunks to the server. The Progress field shows the number of

chunks the server has successfully processed vs the total number. Typically what happens is that the agent finishes importing from AD before the server imports all the chunks. This shows at a minimum that there is progress.

Azure AD Imports

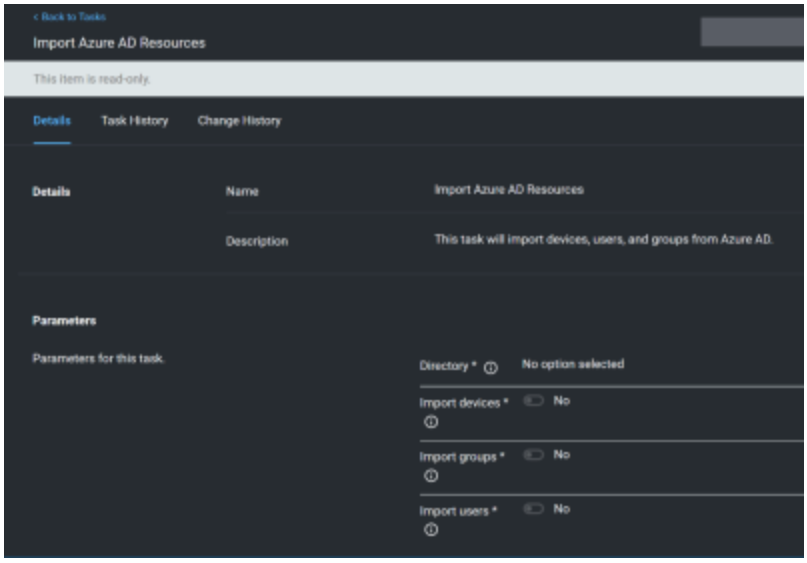
The primary reason for imports from Azure AD is to configure authentication in Privilege Manager.

Users/Groups

Importing users and groups from Azure AD works well for authentication, and usually plays well with data from other sources.

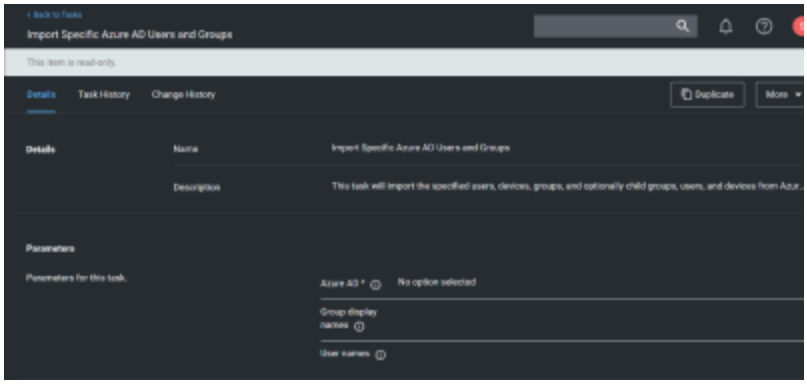
Import Azure AD Resources

This is the primary task users should run to import from Azure AD.



Import Specific Azure AD Users and Groups

This task allows users to import selected users and groups, instead of importing all.



Note: For groups the search filter is by display name. For users either display name or UPN can be entered (or a partial with *). This is a common point of trouble - users often use account names or other names that don't match the Azure AD data. When in doubt, open the Azure AD portal and make sure the display names match.

Device Import

At this time, importing devices (computers) from Azure AD is discouraged. The usable data for Privilege Manager is very limited, and there is basically only one way to link an Azure AD device to an existing computer resource in Privilege Manager and that by Device ID. Refer to Azure AD - Device ID in "Agent Registration" on page 585. Unless the agent is reporting this data, there are guaranteed to be duplicates and/or resources that will not work to assign policies.

On-Premises vs. Cloud

Since Azure AD is itself a cloud service, there's basically no difference between our support on-premises and in cloud.

Thycotic One and Privilege Manager

Overview

Thycotic One is the single-sign-on provider for Delinea applications. With Thycotic One, one user account can be granted access to multiple Delinea products, such as Secret Server, Privilege Manager,DevOps Secrets Vault, and Account Lifecycle Manager.

Thycotic One enables login integration using the OpenID Connect protocol, an industry standard single-sign-on method.

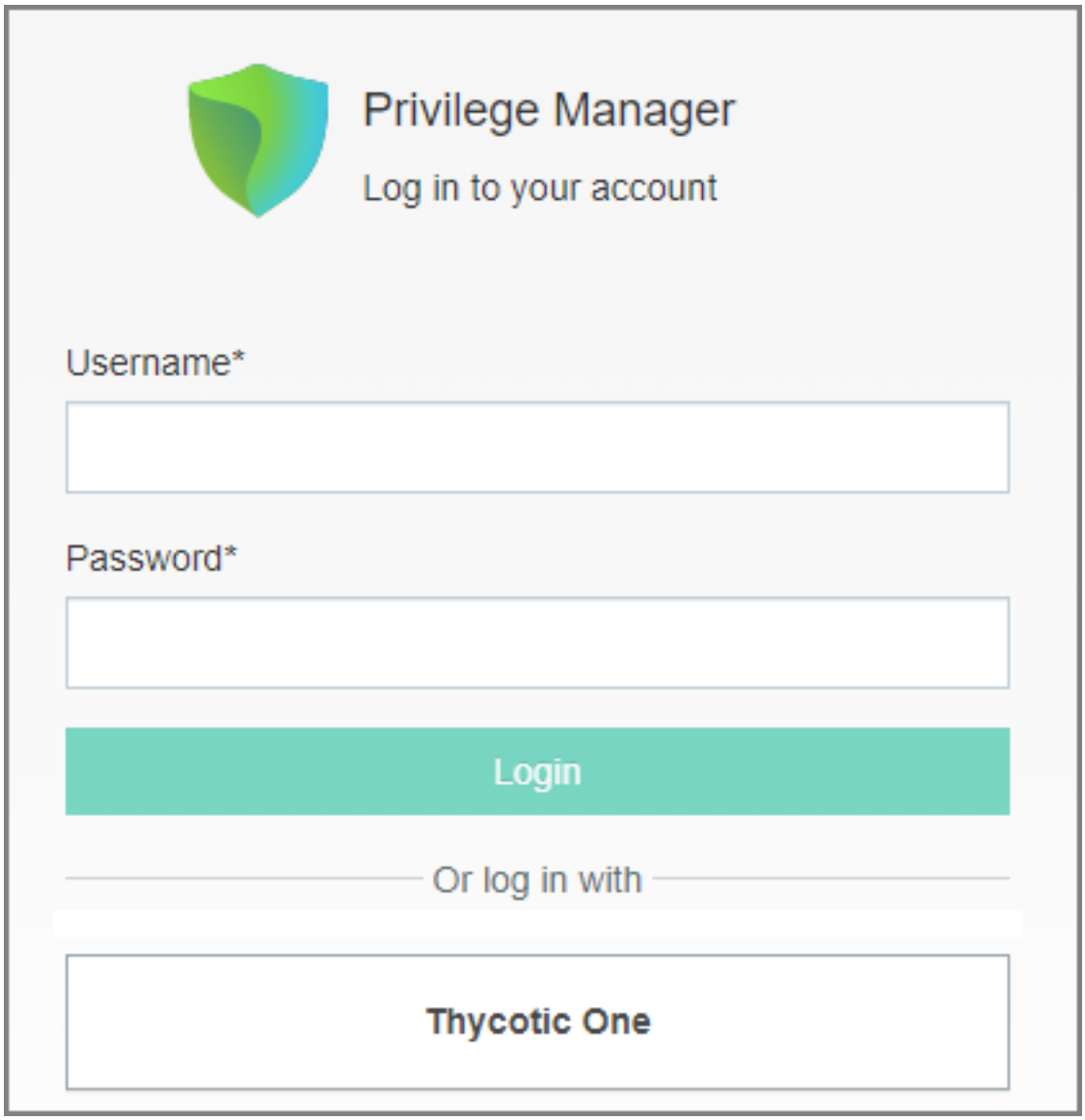
Thycotic One is the default identity provider in Privilege Manager Cloud (PMC). When you set up the cloud instance, it will already be configured and ready to use Thycotic One. The initial admin user will log in with their Thycotic One account, and optionally, all newly created Privilege Manager accounts can be synchronized with Thycotic One, so they can log in that way as well.

Logging in with Thycotic One

When Thycotic One integration is turned on, all Privilege Manager users can log in either with their local passwords or with Thycotic One. All Privilege Manager permissions and configuration will apply to that user regardless of how they logged in.

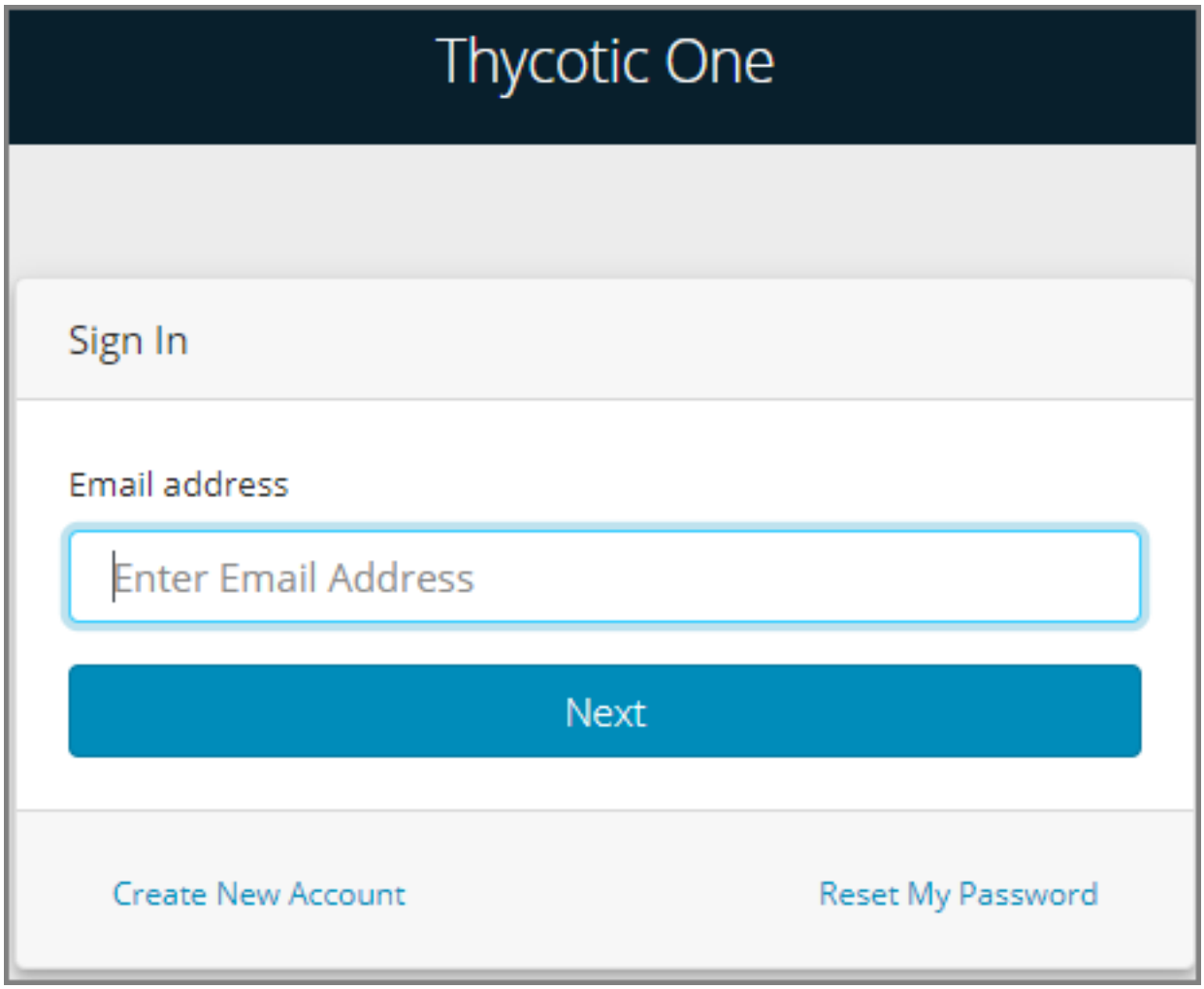
However, the local username and password and the Thycotic One username and password are not necessarily the same thing. In Thycotic One, you'll log in with your email address rather than your username, and the password you use may very well be different from the Privilege Manager password.

You'll see this on the login page:



Clicking **Local Login** will bypass Thycotic One and allow the user to log in with their local Privilege Manager password. Clicking **Thycotic One** will redirect the user to Thycotic One to authenticate. Once that is successfully done, the user will be redirected back to Privilege Manager.

After clicking **Thycotic One**, users will type their email address and password:



And then be redirected back to their dashboard in Privilege Manager.

Configuring Thycotic One as a Foreign System

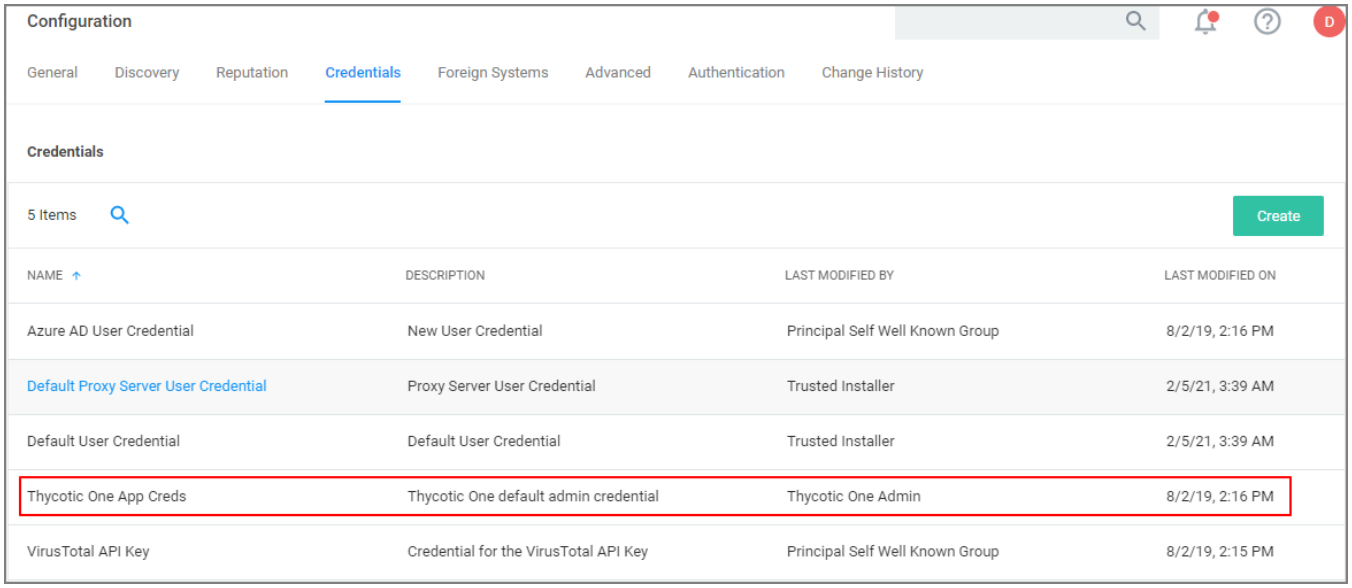
Thycotic One related configuration details can be accessed under **Admin | Configuration**. Two items can be customized:

- Credential: This credential is used by the Thycotic One Foreign System.
- The Thycotic One Foreign System.

Editing up the Credential

1. Navigate to **Admin | Configuration**.
2. Select **Credentials**.
3. Click **Create** to create a new credential to use with Thycotic One or edit details on the existing one. Make sure to provide the correct Thycotic One account name and password information.
4. Click **Save Changes**

Your Thycotic One credential is listed on the **Credentials** tab.

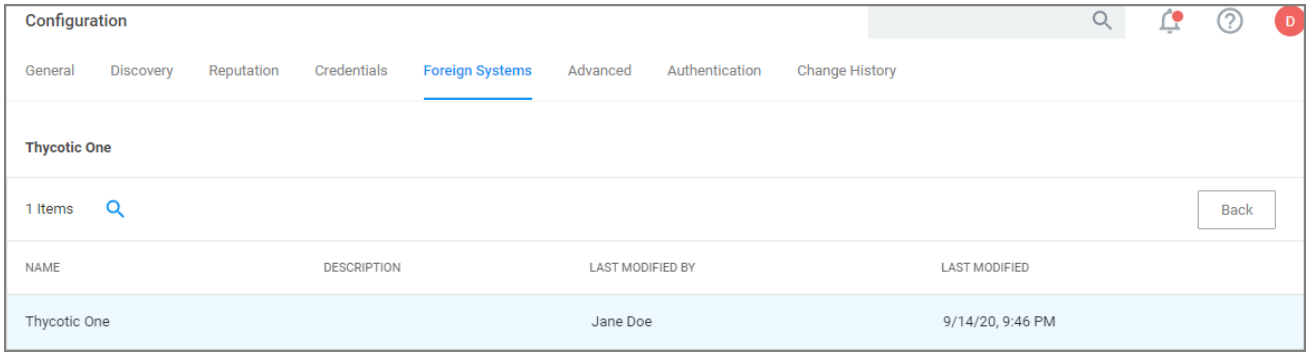


Editing the Foreign System

The Thycotic One Foreign System entry is auto-populated based on the information provided during the registration process as documented in the Cloud Quickstart Guide.

The following steps show how to access the foreign system for edits.

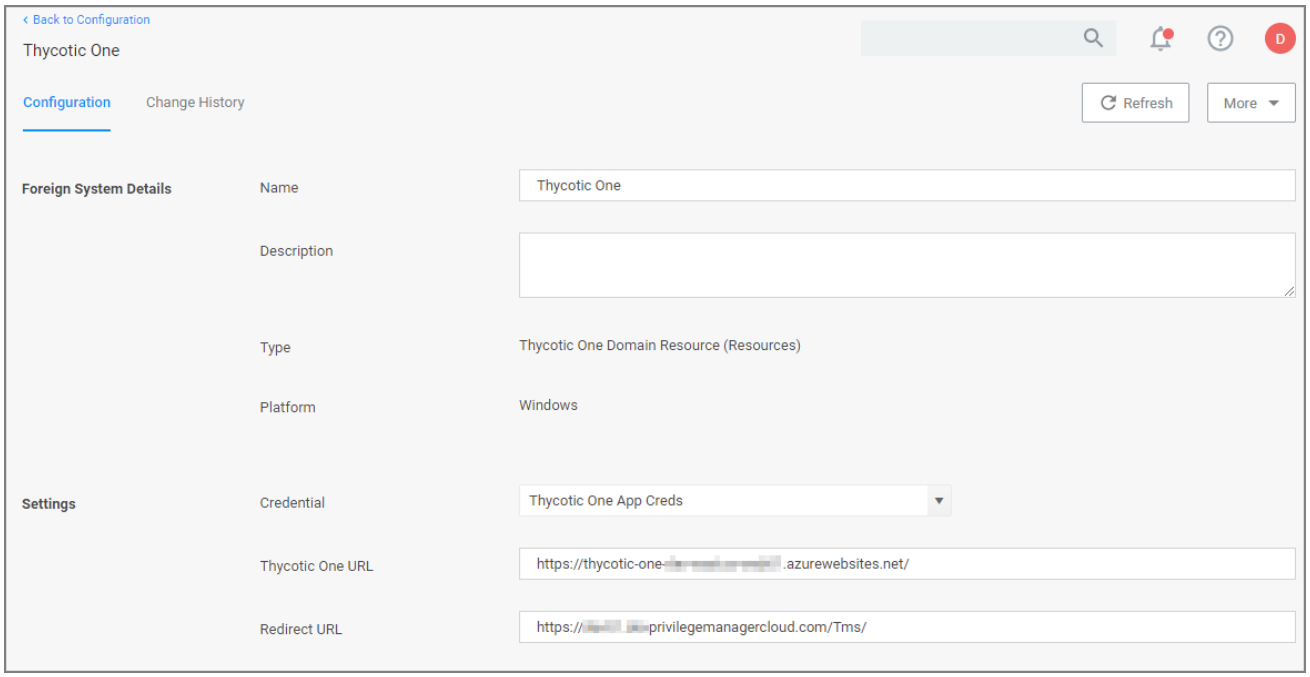
1. Navigate to **Admin | Configuration**.
2. Select **Foreign Systems**.
3. Select **Thycotic One**.



4. Customize the Name and Description.
5. Under **Settings** you may edit:
   a. **Credential**: This is the name of the credential that you created for Thycotic One based on the previous procedure.
   b. **Thycotic One URL**: This is the URL forThycotic One that is based on the region selection during the setup

process.

c. **Redirect URL**: This is the URL to your specific Privilege Manager Cloud instance.



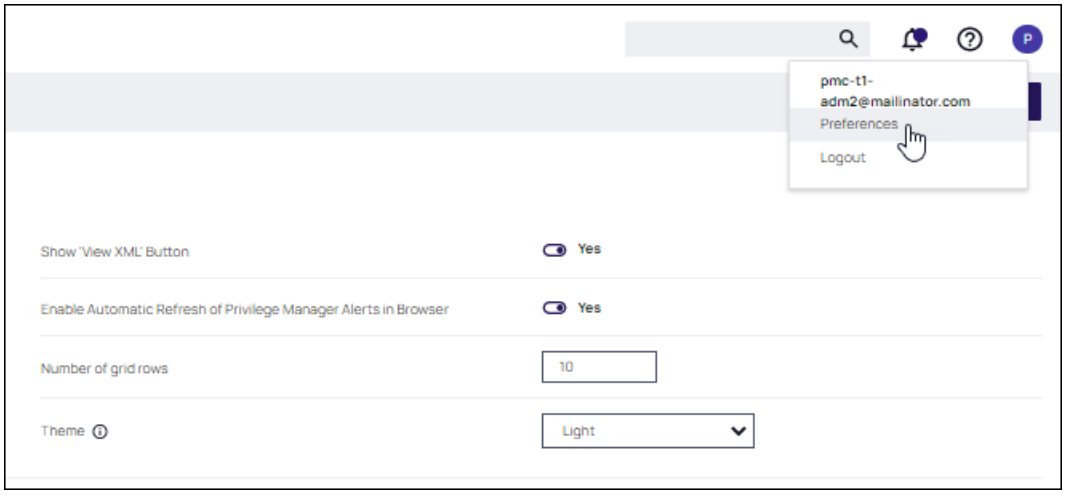
Deleting a Thycotic One Account (pre v11.4.0)

Thycotic One user accounts created in v11.4.0 and later have the **Delete** action available in the user interface without editing the account's XML. Refer to Editing, Deleting, and Exporting a User.

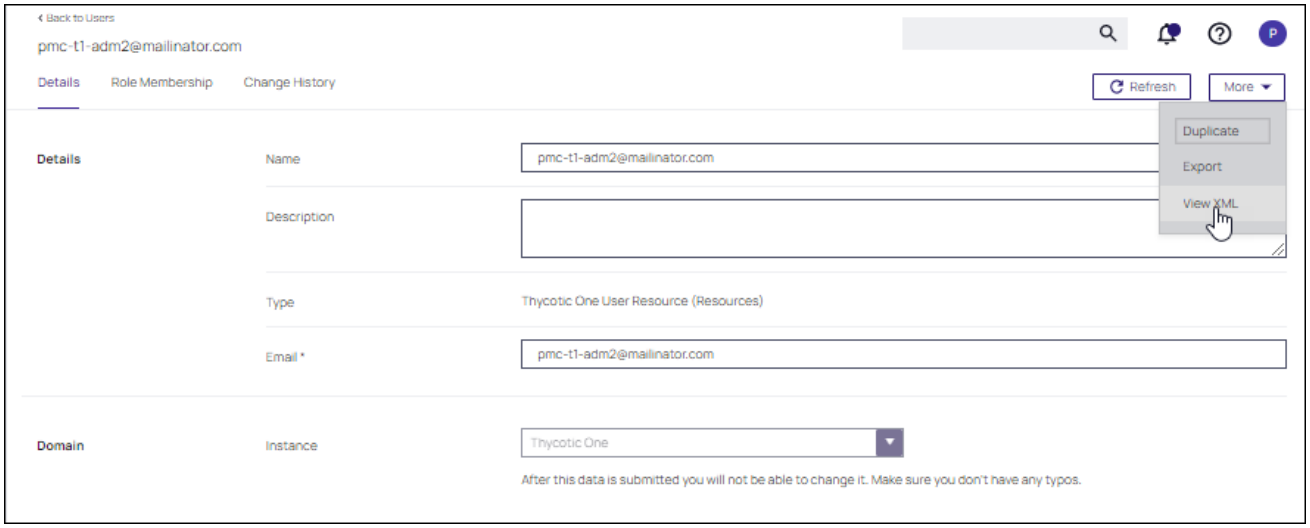
For user accounts created prior to v11.4.0, follow these steps to edit the account's XML and enable the **Delete** action in the user interface for those accounts.

Note: Thycotic One accounts in Privilege Manager Cloud should first be removed from the Product membership in the Thycotic One portal manager. Additionally, Thycotic One accounts, that are the only accounts that have access to a Privilege Manager Cloud instance in situations when authentication from Azure/SAML, may be broken (expired keys, application tenant expiration, etc.,).

1. In your user preferences, make sure that **Show XML** is enabled.



2. Select **Admin** | **Users**, select the Thycotic One user.
3. In the upper right, click **More** and select **View XML**.



4. In the XML Editor, click the **Edit** button. Remove the attribute **NoDelete** (line 2).

5. Select **Import** then **Save** the XML.

6. Return to the user details for the Thycotic One account. Click **More** and the option to **Delete** is available.

Delinea Products Integrations

The following topics on integrating Privilege Manager with other Delinea products are available:

- Integrating with Secret Server
- Integrating with PrivilegedBehaviorAnalytics
- Thycotic One and Privilege Manager Cloud

Integrating with Privileged Behavior Analytics

Delinea's Privileged Behavior Analytics (PBA) SaaS product can be integrated with Privilege Manager cloud instances

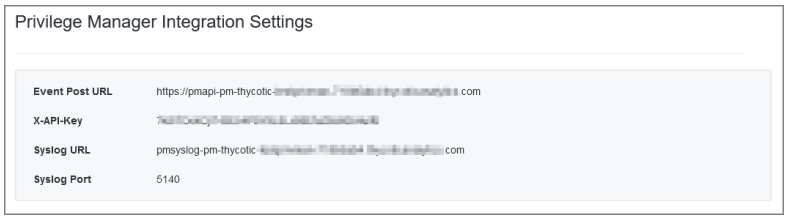
For the integration to work correctly independent of your Privilege Manager instance, you need to have a Delinea enabled PBA instance.

Refer to the PBA Documentation for details on features and functionality of PBA.

PBA System Settings Details

You will need to retrieve the PBA System Settings details required for setting up the integration in Privilege Manager.

1. Navigate to the **PBA Systems Settings** page (/system_settings/).



2. Use the Syslog URL and port information when setting up the **SysLog Foreign System** below. Use the Event Post Url and the X-API-Key when setting up the **Send Application Events to PBA** below.

Setting Up PBA Integration on Privilege Manager

Required PBA resources are provided via Privilege Manager Configuration Feeds.

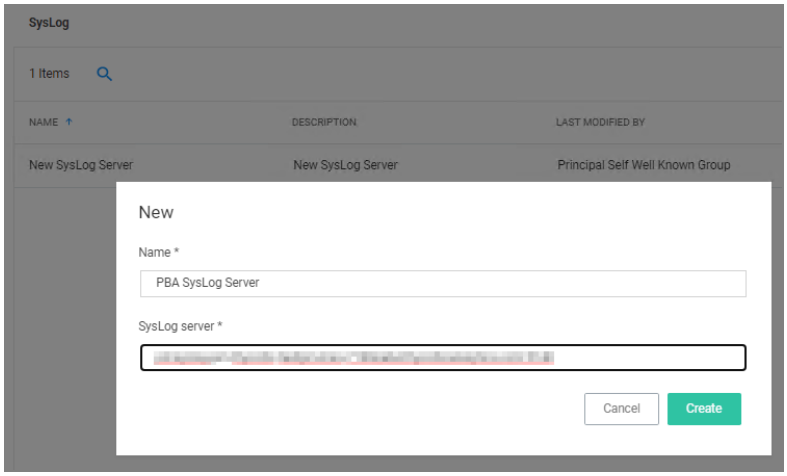
Downloading and Installing the PBA Config Feed

1. In you Privilege Manager console, navigate to **Admin | Config Feeds**.
2. Expand **Privilege Manager Product Configuration Feeds**.
3. Expand **Thycotic Management Server Core**.
4. Install **Privileged Behavior Analytics Integration**.

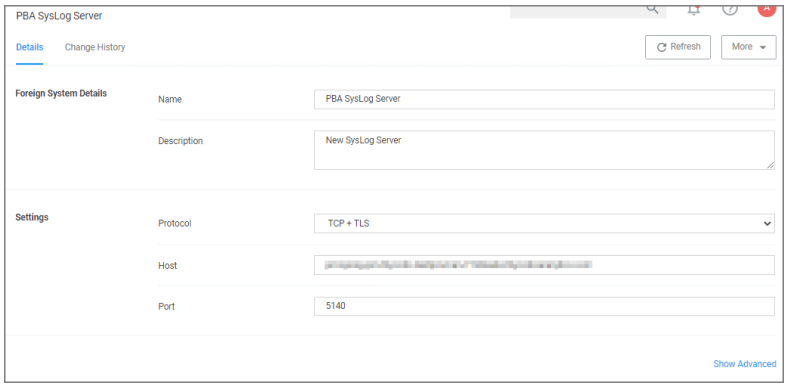
After the install, proceed to the Foreign Systems setup.

Setting up the PBA SysLog Foreign System

1. Navigate to **Admin | Config** and select **Foreign Systems**.
2. Select **SysLog**.
3. Click **Create**.
4. Enter a name and your SysLog server details.

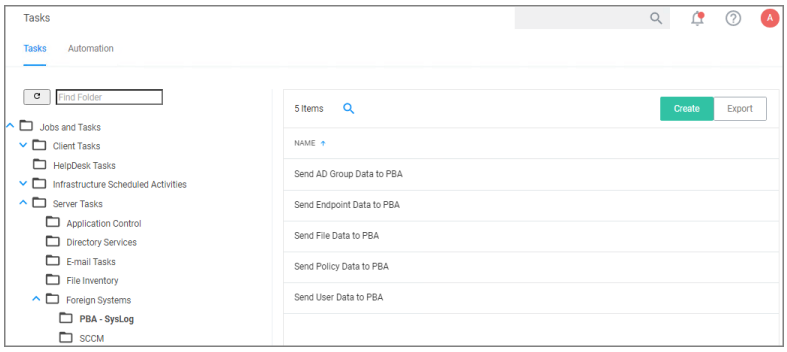


5. Click **Create**.
6. Verify that your Protocol, Host, and Port match your SysLog server details (SysLog URL and SysLog Port from the PBA System Settings details).

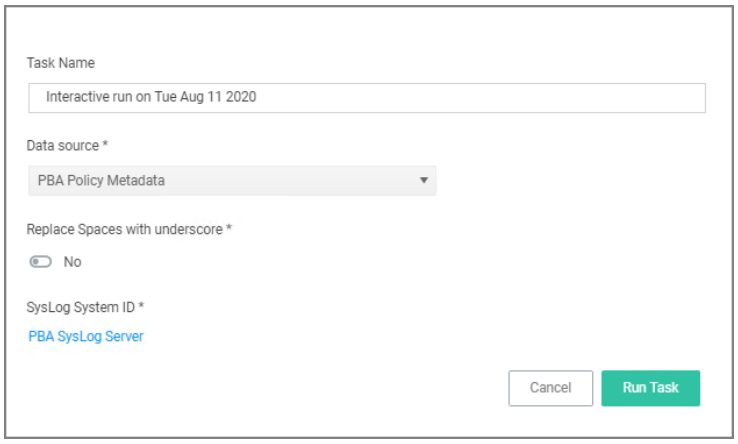


Using the PBA Send Tasks

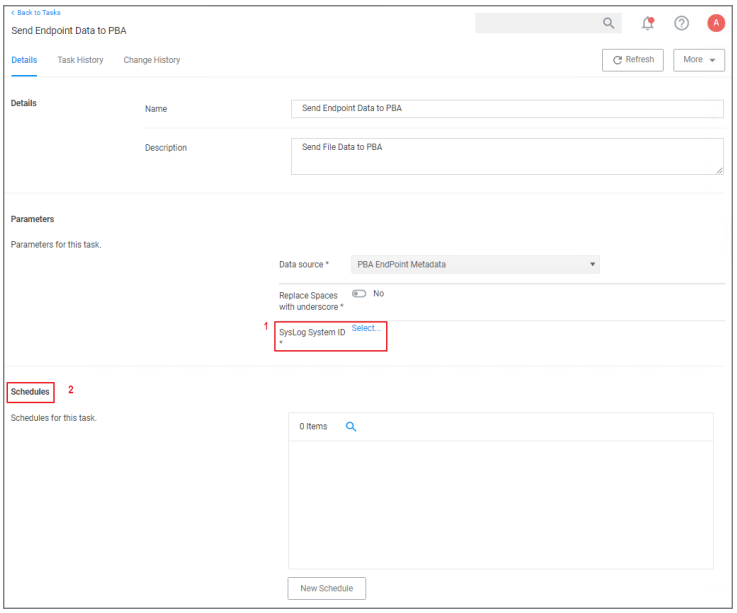
1. Navigate to **Admin | Tasks** and from the folder tree select **Server Tasks | Foreign Systems**.
2. Click **PBA - SysLog**.



3. For Privilege Manager to send data based on any of these task, the PBA SysLog server you created as a Foreign System above, needs to be added as the SysLog System ID. This can either be done
   - **On Demand** when running the task:
     a. Select a PBA Data Send tasks and click **Run**.
     b. Specify the SysLog System ID.



     c. Click **Run Task**.
   - **By setting up a schedule**:
     a. Select a PBA Data Send tasks and click **View**.
     b. Under **Parameters** specify the SysLog System ID.
     c. Define a **Schedule**, by clicking **New Schedule**



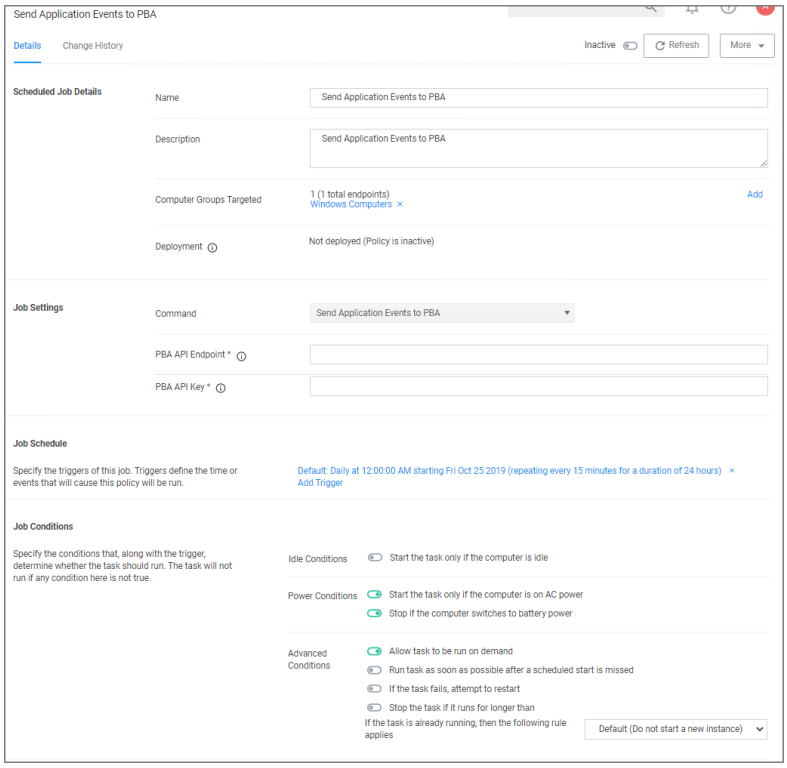
d. Click **Save Changes**.

Repeat for each of the data sets you want to use in PBA.

Enable Send Application Events to PBA

The config feeds installation also add a remote scheduled client command for PBA to Privilege Manager. The **Send Application Events to PBA** policy is by default disabled.

1. Under your computer Group navigate to **Scheduled Jobs**.
2. On the **Scheduled Jobs** page search for PBA and select **Send Application Events to PBA**.



- Under Job Settings enter the PBA **Event Post URL** and **X-API-Key** details from the PBA system settings information.
- Modify the Job Schedule if customization is required.
- Customize any of the Job Conditions to better fit your implementation.

3. Click **Save Changes**.
4. Set the **Inactive** switch to **Active**.
5. Next to Deployment click the **i** icon and select the **Resource and Collection Targeting Update** task to run.

Integrating Privilege Manager and Secret Server

The integration with Secret Server provides the ability to use Secret Server in either of two ways:

- Authentication: When usingSecret Server for authentication, you can login to Privilege Manager with users that are created and managed in Secret Server.

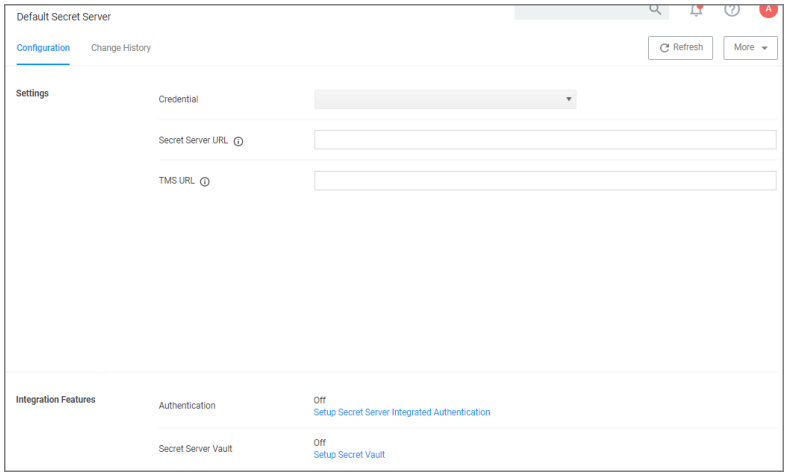
  Note: The Secret Server and Privilege Manager integration for authentication purposes is not support in cloud instances. It is only supported for Privilege Manager on-premise.

- Vaulting: Customers can choose to integrate with Secret Server Vault. In Secret Server, Privilege Manager credentials are stored as secrets, and Privilege Manager uses the Secret Server REST API to communicate with Secret Server.

Setup the Integration

Note: Proper license types need to be set-up, as Secret Server Express (free) does not support the integration with Privilege Manager.

1. Navigate to **Admin | Configuration**.
2. If you do not have a Secret Server vault configured, click the **Advanced** tab. In the **General** section, locate the **Secret Server Vault** parameter and click **Configure**. Provide the required parameters and click **Save Changes**.
3. Click the **Foreign Systems** tab.
4. Select **Secret Server** from the list.
5. In the **Name** column, click on **Default Secret Server**.



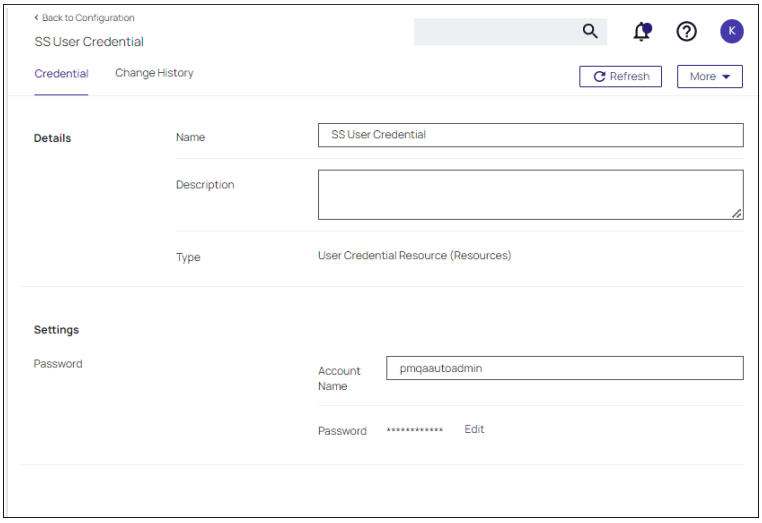
6. Under Settings, update the following:
   - **Credential**: This is a Secret Server user (preferably an application account). Refer to required permissions above. If you need to obtain credentials, in your Secret Server application, navigate to **Admin | Users** and verify you have a user configured to be used for the credential setup in Privilege Manager. This can be a regular Secret Server user or aSecret Server Application account.

     Note: An Application account is recommended. The account needs to have a role with ALL of the following Secret Server permissions.

     - Add Secret
     - Administer Configuration
     - Administer Folders
     - Administer Licenses
     - Assign Secret Policy
     - Create Root Folders
     - Delete Secret

- Edit Secret
- wn Secret
- View Secret

In your Privilege Manager instance, enter the credentials for that user at **Admin | Configuration | Credentials**. Create/edit the defaultSecret Server credential account to specify which account will be used by Privilege Manager to connect to Secret Server. Depending on your setup, this can be the **Default User Credential** in Privilege Manager.

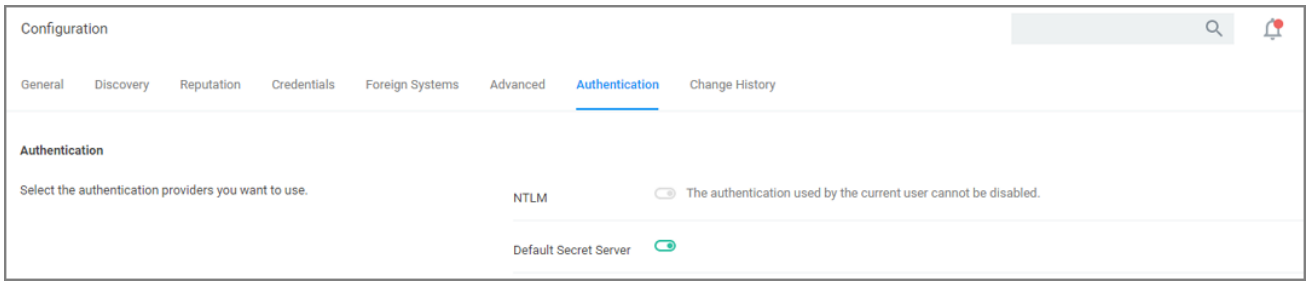


- **Secret Server URL**: This is the URL that end users use to access Secret Server. **HTTPS** is required. Also, the validation on this field reaches out toSecret Server using the URL provided. If it can't be reached, or if theSecret Server version is lower than v10.6, there will be a 404 not found validation error. The URL needs to be fully qualified ending with a /.
- **TMS URL**: This is the URL to access TMS itself. It is the URL that end users use to access Privilege Manager, minus the `PrivilegeManager/` part at the end of the path. This URL also needs to be well formed and fully qualified ending with a `/`.

7. Click **Save**.

Integrating with Secret Server for Privilege Manager Authentication

1. Scroll down to **Integration Features | Authentication** and enable Secret Serveras the authentication provider by clicking the **Setup SecretServer Integrated Authentication** link.
2. Set the switch for Secret Server to enabled.



3. Click **Save Changes**.

   After these steps the Secret Server Foreign System is ready for use.

Integrating with Secret Server Vault to Store Secrets

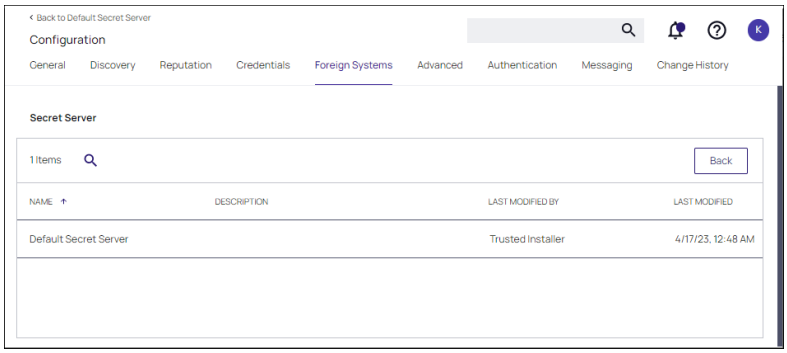
This method of vaulting, allows passwords created in Privilege Manager (user credentials, rotating passwords for agents, etc.) to be stored and maintained in Secret Server as secrets.

Documentation for Secret Server can be found at `https://docs.delinea.com/online-help/products/secrets/current`.

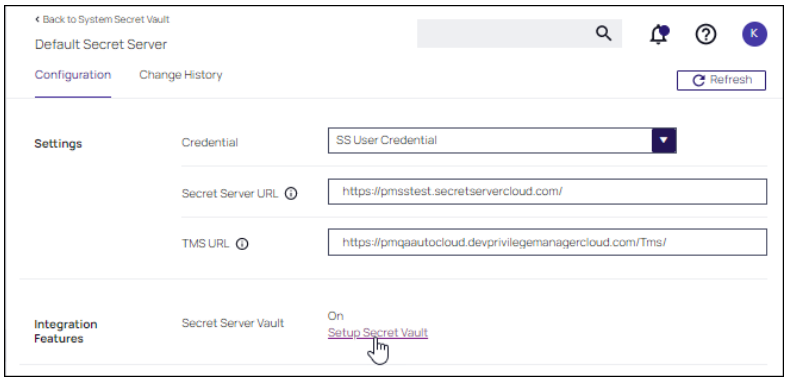
1. In Secret Server, verify Web Services are enabled. Webservices can be enabled at the **Administration** > **Configuration** in the **General** tab.

   Verify that under View Webservices the **Enable Webservices** option is reflecting **Yes**.

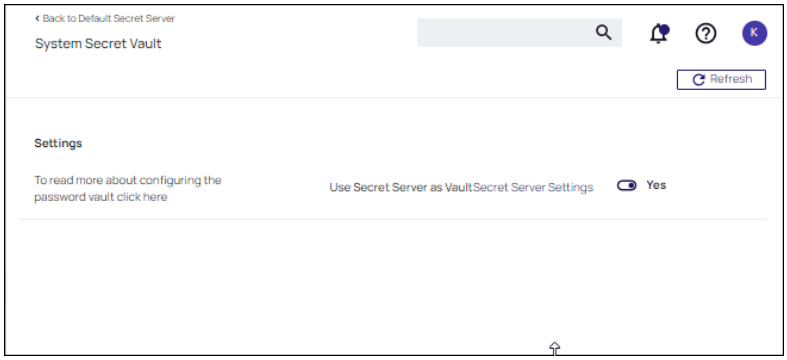
2. In your Privilege Manager instance, select your Secret Server instance on the **Foreign System** tab at **Admin** | **Configuration**.



3. Scroll down to **Integration Features | SecretServer Vault** and setupSecret Server as the vault by clicking the **Setup Secret Vault** link.



4. Set **Use Secret Server as Vault** to **Yes**. You are prompted to backup the Secret Server database. Once confirmed, a task is automatically scheduled to start migrating the secrets.



Password Migration

After the vault and authentication set-up, all passwords are migrated from Privilege Manager to Secret Server. This migration process may take time.

Important Notes

The migration will create a root folder in Secret Server named Privilege Manager Secrets. Do NOT delete this folder. The folder, by default only has the sync account user as an owner, with no other permissions. The permissions on this folder can be modified to allow help desk users or administrators access to the Secrets. Do NOT remove the sync account user's permissions from the folder.

If desired, the folder can be moved or renamed within Secret Server.

Templates

There are two Templates that Privilege Manager uses to store Secrets in Secret Server. These templates must exist with the proper fields and be marked as active.

- **Password (Template Id: 2)**: The following fields need to exist on the template:
  - **Username**
  - **Password**

  Do NOT mark any other fields in that template as required!
- **Windows Account (Template Id: 6003)**: The following fields need to exist on the template:
  - **Machine**
  - **Username**
  - **Password**

  Do NOT mark any other fields in that template as required!

Third-Party Foreign Systems Integration

- Setting up a Cylance Connection
- Setting up a Jamf Connection
- Setting up SAML for SSO
  - GSuite specifics
- Setting up an SCCM Connection
- Setting up a ServiceNow Integration
  - ServiceNow Application
  - Setting up a ServiceNow Webhook
- Setting up the SMP Integration
- Setting up an SMTP Server Connection
- Setting up a Syslog Connection
- Setting up a VirusTotal Connection

Installing Foreign System Connectors

Foreign system connectors are not automatically installed on the Privilege Manager instances. These are the basic steps of installing a connector:

1. Open the Privilege Manager console.
2. Browse to `https://YourInstanceName/TMS/Setup/`.
3. On the **Currently Installed Products** page, Click **Install/Upgrade Products**.
4. Select the connectors you wish to install.
5. Click **Install**. Accept any End User License Agreement if prompted and monitor the installation process for error conditions.

Privilege Manager cloud instances have connectors pre-installed and available for configuration without the need to run through the connector install.

Setting up a Cylance Integration

Cylance is an Artificial Intelligence Based Advanced Threat Prevention Solution for enterprise environments. Privilege Manager (v10.5+) integrates with Cylance to help you proactively act on any unknown applications that run in your environment to prevent potential malware attacks. The steps below walk through how to setup a Cylance Integration in Privilege Manager and then create an example policy to begin using Cylance intelligence in action across your environment.

Keep in mind that while the Cylance integration provides insight into threat analysis, ultimately you can use Privilege Manager policies to act or react in whatever way makes most sense to your organization.

Cylance Connector Installation Steps (On-prem only)

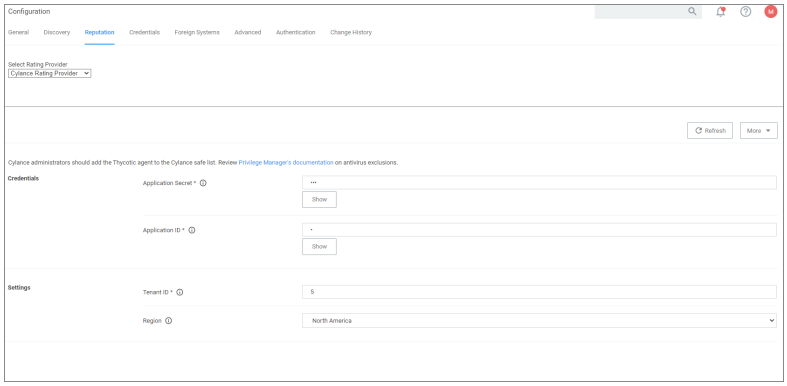
1. Open a browser on your Privilege Manager Web Server, browse to `https://[YourInstanceName]/TMS/Setup/`.
2. On the Currently Installed Products screen, choose Install/Upgrade Products.
3. Select the **Thycotic Cylance Reputation Connector** option.
4. Click **Install** and accept the End User License Agreement. You will see your Installation Progress. Click on "Show install Logs" link to check for any errors

   Note: If the installation of Cylance initially fails, redirect to https://[YourInstanceName]/TMS/Setup/ and click the Repair button next to the Cylance Product.

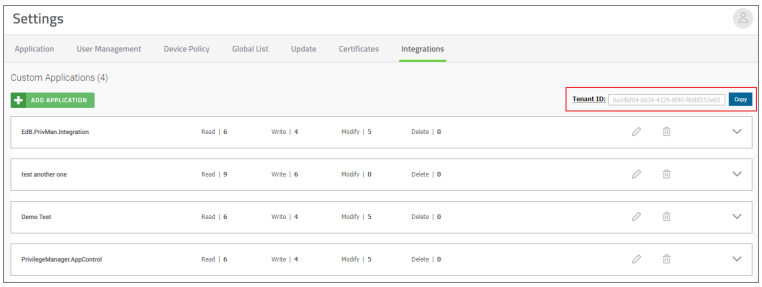
5. Once the Installation is successful, click **Home**.

Configuring the Cylance Connector

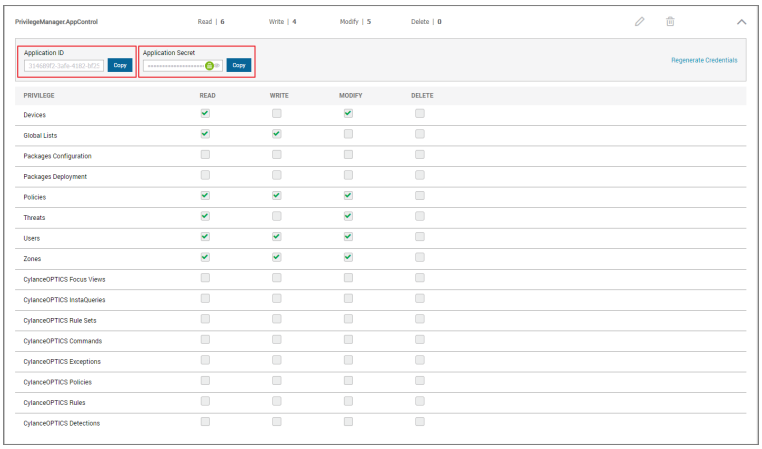
1. Navigate to **Admin | Configuration** and select the **Reputation** tab.
2. From the Select Rating Provider drop-down, select **Cylance Rating Provider**.



3. Enter the required **Credentials** and **Settings** details. These details can be found in your Cylance account (login at protect.cylance.com).
   a. In our Cylance account, navigate to **Settings** and select **Integrations**. You find the **Tenant Id** on the right side of the Custom Applications area.



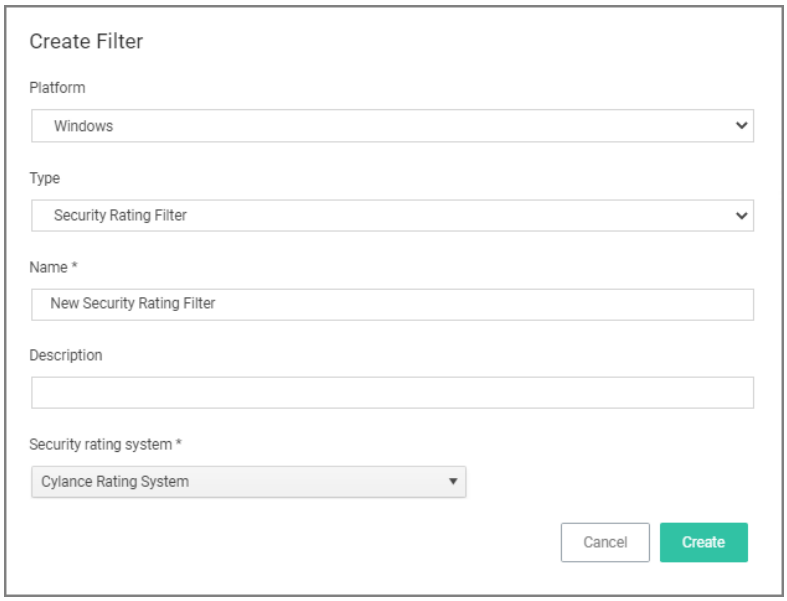
b. Select your Privilege Manager integration from the Custom Application list. You find the required **Application ID** and **Application Secret** on the left side of the page.



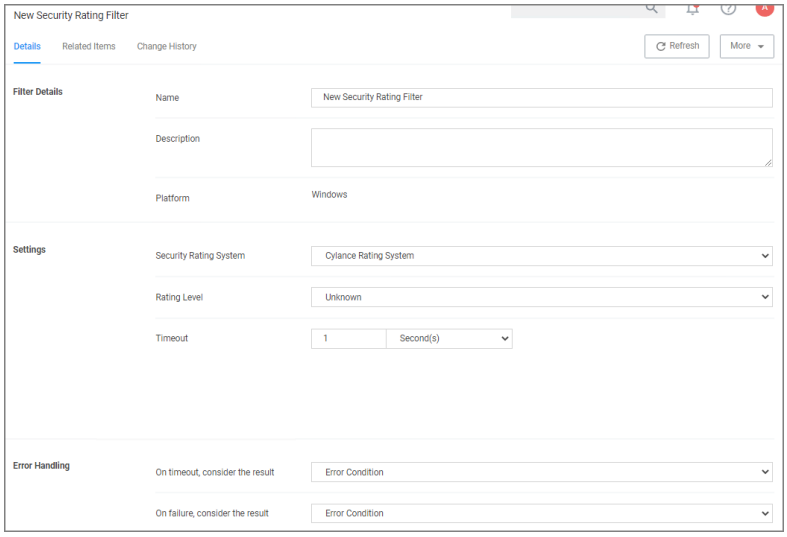
4. Once the Cylance details are entered in Privilege Manger, click **Save Changes**.

Create a Cylance Security Rating Filter

1. Navigate to **Admin | Filters**.
2. Click **Create Filter**.
3. From the **Platform** drop-down select either Windows or macOS.
4. From the **Filter Type** drop-down select **Security Rating Filter**.
5. Name the policy and add a Description.
6. From the **Security Rating System** drop-down, select **Cylance Rating System**.



7. Click **Create**.



8. Click **Create**.
9. Select the **Rating Level** you wish to apply. You can also specify a **Timeout** value and **Error Handling** conditions on timeout and/or on failure, the options are:
   - Matched
   - Not Matched
10. Click **Save Changes**.

Create a Cylance Policy

Use the Application Policies wizard to create a policy that uses the Cylance Security Rating filter created in the steps above.

Setting up a Microsoft System Center Configuration Manager (SCCM) Integration

Privilege Manger integrates with Microsoft System Center Configuration Manager (SCCM) to allow the

- import of computers for use in computer groups and identifying systems that exist on the network, but don't have an endpoint agent installed yet.
- import of existing Device Collections from SCCM and use them for Privilege Manager computer groups.
- inventory of SCCM Software Packages to use the package contents in Privilege Manager Application Control policies.

Create a Credential

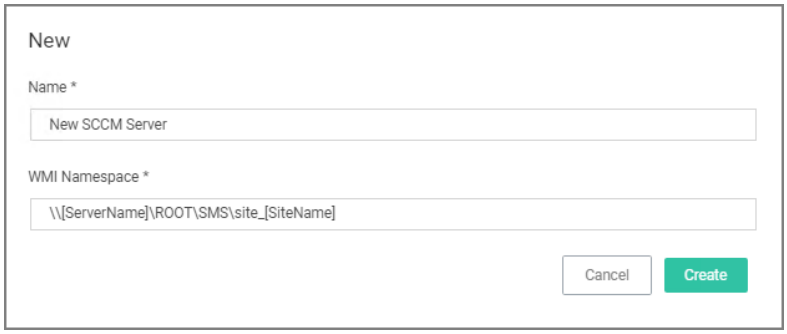
Privilege Manager needs a username and password to access SCCM. If you have not already created an appropriate user credential:

1. Navigate to **Admin | Configuration | Credentials**.
2. Click **Create**, to create user credentials to access SCCM.
3. After entering the user credentials information for SCCM, click **Save Changes**.

Connecting to SCCM

Before you can import data from SCCM you need to setup a foreign systems connection in Privilege Manager for the SCCM integration.

1. Navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
2. Select **System Center Configuration Manager**. If this is not listed, make sure the connector is installed by verifying via the **Privilege Manager Add/Upgrade Features** page.
3. Click **Create**.

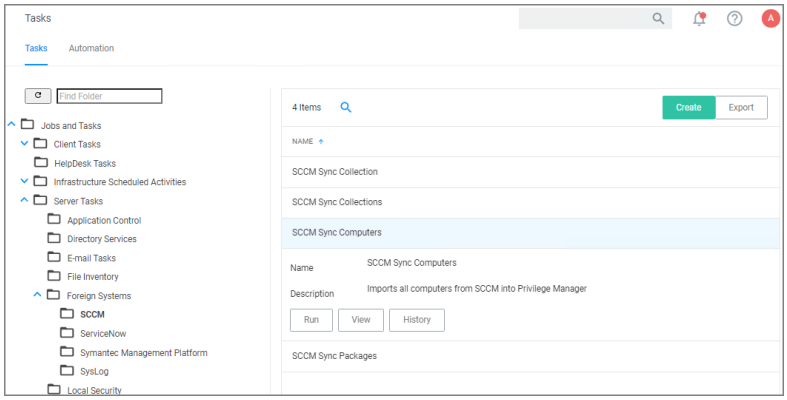


4. Enter the name of the SCCM Server and provide the **WMI Namespace of the SCCM Site**.
5. Click **Create**.
6. Under Settings from the **Credential** drop-down, select the SCCM account created in the previous procedure.
7. Click **Save Changes**.

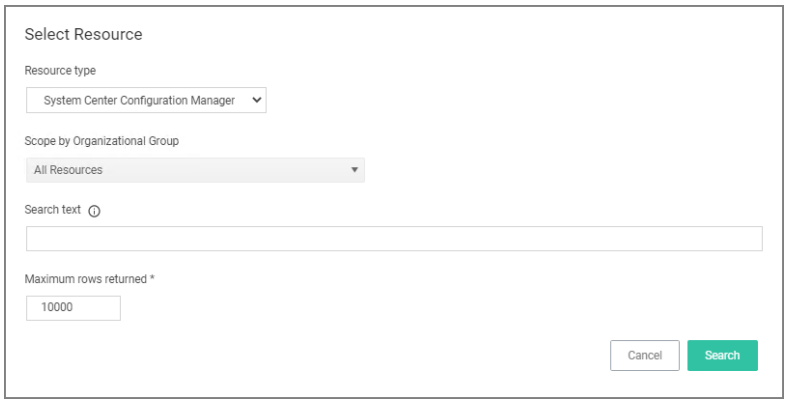
Import Computers

Before you can import collection data from SCCM, Privilege Manager needs to know about computers in your SCCM.

1. Navigate to **Admin | More** and select **Tasks**.
2. On the Tasks tab open the folder tree and select **Server Tasks | Foreign Systems | SCCM**.
3. Click **SCCM Sync Computers**.



4. Click **Run**.
5. Select your SCCM system via the **Select...** option.



   a. Under Scope by Organizational Group type the name of your sccm system in the search text or use the search option.

6. Click **Run Task**.

Verify the Computers have been Imported (optional)

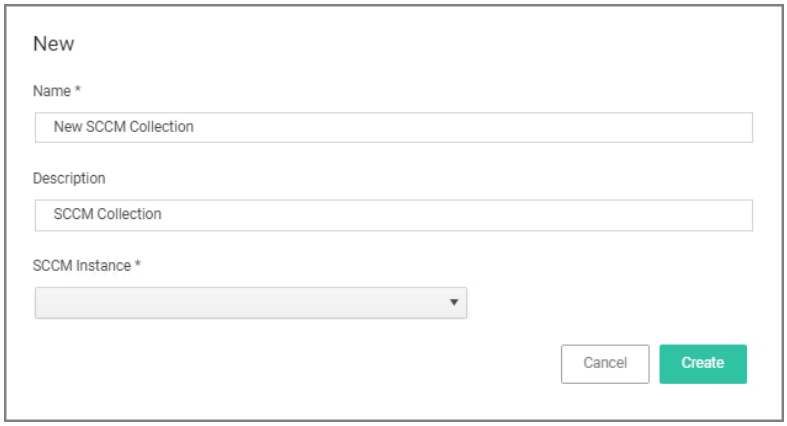
1. Navigate to **Admin | Resources**.
2. Open the **Resources** tab.

3. In the folder tree open **Organizational Views | Default | All Resources | Asset | Network Resource | Computer**.
4. Select a computer from that list.
5. Select the Known Data tab in the computer resource explorer view.
6. In the tree under **Foreign Systems**, you should have the Foreign System Id and SCCM Platform Id data.

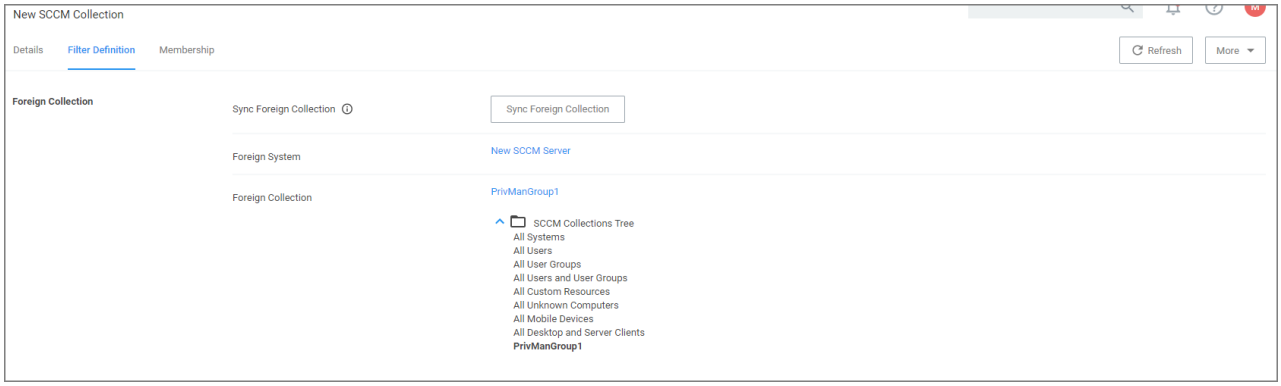
Create a Collection

After computers have been imported, you can create a collection to mirror an SCCM collection.

1. Navigate to **Admin | Resources**, open the **Resource Filters** tab.
2. In the folder tree under **Resource Filters** open **Collections | System Center Configuration Manager**.
3. Click **Create**
4. Enter a Name and Description, and specify the SCCM instance to connect to.



5. Click **Create**.
6. Select the Filter Definition tab and under **Foreign Collection** select the Collection target.



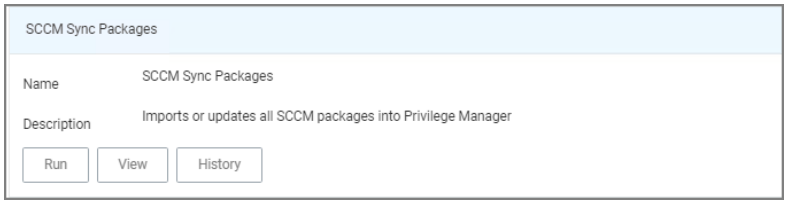
7. Click **Save Changes**.

8. Click the **Sync Foreign Collection** to update the membership immediately. The foreign collection update can also be scheduled by following the link in the help tip.
9. Select the Membership tab and then click the **Update Membership** tab to see the current membership of this collection.

Inventory Software Packages

Once the Foreign System has been created, an on-demand packages synchronization can be run and/or a regular synchronization schedule can be set-up via the following steps:

1. Navigate to **Admin | More** and select **Tasks**.
2. On the Tasks tab open the folder tree and select **Server Tasks | Foreign Systems | SCCM**.
3. Click **SCCM Sync Packages**.



4. Click **Run**.
5. Select your SCCM system via the **Select...** option.
   a. Under Scope by Organizational Group type the name of your sccm system in the search text or use the search option.

6. Click **Run Task**.

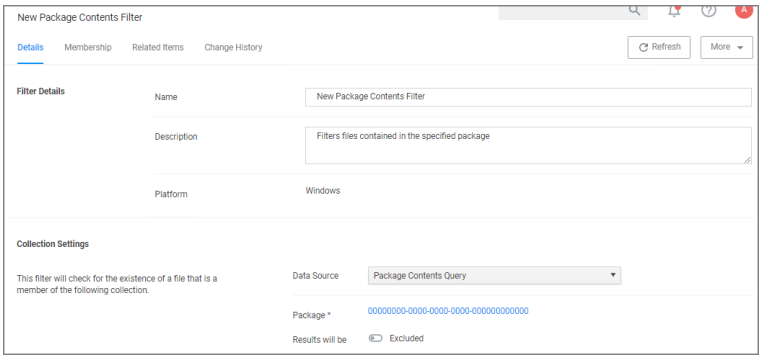
Alternatively the **SCCM Sync Packages** task can be scheduled to regularly repeat. When viewing the task, navigate to the Schedules tab and create a new schedule.

Create a SCCM Package Content Filter

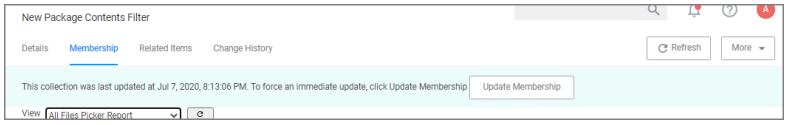
After the Package Synchronization completes the SCCM Packages can be used in application control policies via package content filters.

1. Navigate to **Admin | Filters**.
2. Click **Create Filter**.

3. From the Platform drop-down select Windows.
4. From the Filter Type drop-down scroll to Inventory Filters and select the **Package Contents Filter**.
5. Set the Name and Description of the filter.
6. Click **Create**.
7. Under **Collection Settings**
   a. from the **Data Source** drop-down select a resource.
   b. Click the package link to specify the SCCM that will be targeted.
   c. Set the switch **Results will be** to **Included**.



8. Navigate to the **Membership** tab.
9. If no items are listed in the membership table, click **Update Membership**.



   Running the sync package task, causes the server to inventory the package referenced in the filter. If you have multiple filters and packages, Delinea recommends to use the *Inventory Packages Referenced in Allowlists* task instead.

10. Click **Save Changes**.

This filter can then be referenced in Application Control policies.

Setting up a ServiceNow Integration

With Privilege Manager v11, a Delinea Privilege Manager ServiceNow application is available in the ServiceNow store combining the power of a ServiceNow approval workflow and Privilege Manager's application execution and elevation application control.

Refer to the instructions in the Integrations documentation.

Setting us a Symantec Management Platform (SMP) Integration

Privilege Manger integrates with the Symantec Management Platform (SMP) to allow the

- import of computers for use in computer groups and identifying systems that exist on the network, but don't have an endpoint agent installed yet.
- import of existing Resource Collections from SMP and use them for Privilege Manager policy targets.
- inventory of SMP Software Packages to use the package contents in Privilege Manager Application Control policies.

Create a Credential

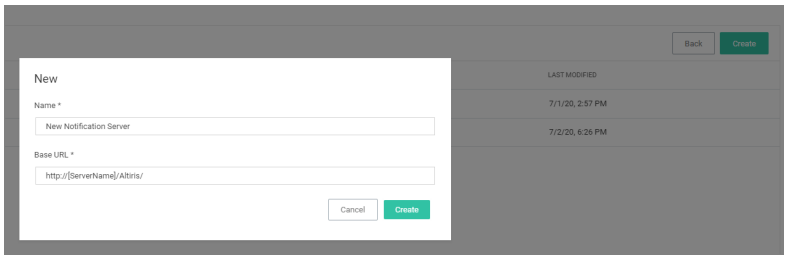
Privilege Manager needs a username and password to access SMP. If you have not already created an appropriate user credential:

1. Navigate to **Admin | Configuration | Credentials**.
2. Click **Create**, to create user credentials to access SMP.
3. After entering the user credentials information for SMP, click **Save Changes**.

Connecting to SMP

Before you can import data from SMP you need to setup a foreign systems connection in Privilege Manager for the SMP integration.

1. Navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
2. Select **Symantec Management Platform**. If this is not listed, make sure the connector is installed by verifying via the Privilege Manager Add/Upgrade Features page.
3. Click **Create**.

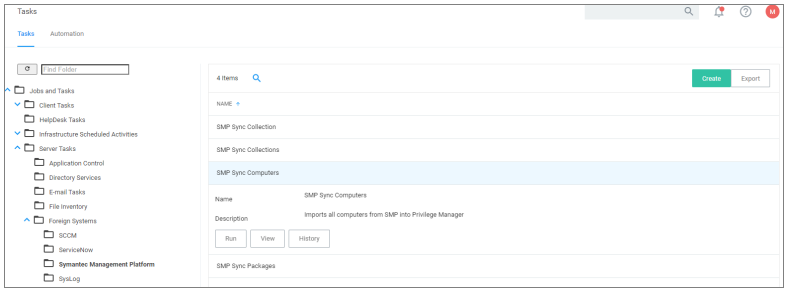


4. **Name** the Symantec Management Platform and provide the **URL of the Altiris console**.
5. Click **Create**.
6. Select the newly created SMP foreign system and click **Edit**.
7. Under Settings select the SMP user credential that you created in the previous procedure.
8. Click Save.

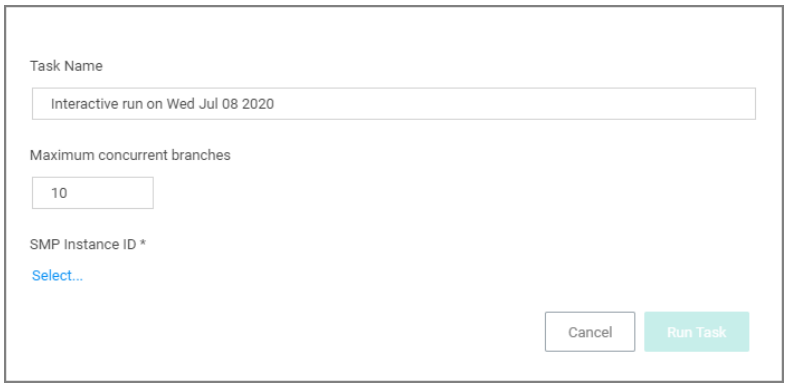
Import Computers

Before you can import collection data from SMP, Privilege Manager needs to know about computers in your SMP.

1. Navigate to **Admin | Tasks**.
2. On the Tasks tab open the folder tree and select **Server Tasks | Foreign Systems | Symantec Management Platform**.
3. Click **SMP Sync Computers**.



4. Click **Run**.
5. Select your SMP system via the **Select...** option.



6. Click **Run Task**.

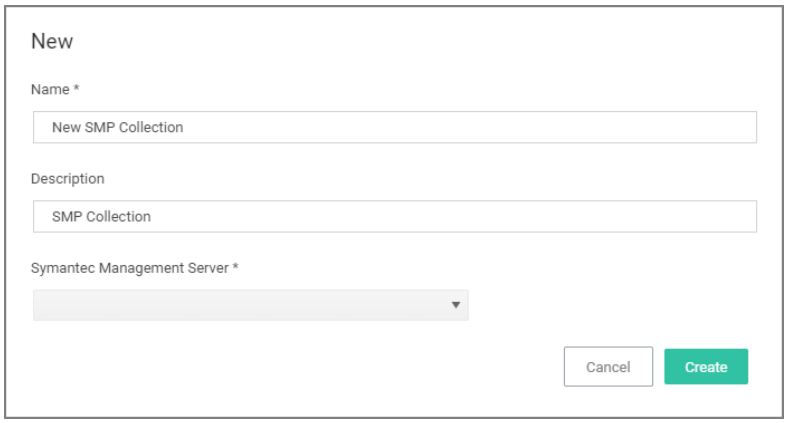
Verify the Computers have been Imported (optional)

1. Navigate to **Admin | Resources**.
2. Open the **Resources** tab.
3. In the folder tree open **Organizational Views | Default | All Resources | Asset | Network Resource | Computer**.
4. Select a computer from that list.
5. Select the Known Data tab in the computer resource explorer view.
6. In the tree under **Foreign Systems**, you should have the Foreign System Id and SMP Platform Id data.

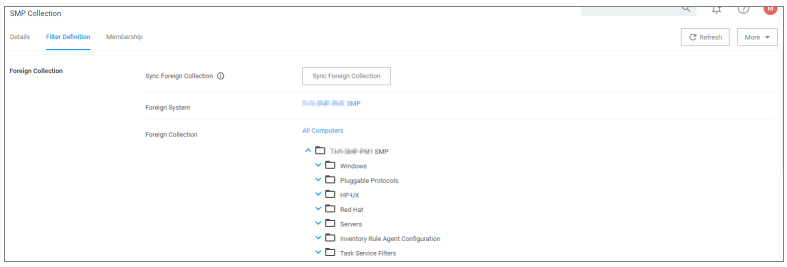
Create a Collection

After computers have been imported, you can create a collection to mirror an SMP collection.

1. Navigate to Resources, open the **Resource Filters** tab.
2. In the folder tree under **Resource Filters** open **Collections | Symantec Management Platform**.
3. Click **Create**
4. Enter a Name and Description, and specify the SMP instance to connect to.



5. Click **Create**.
6. Select the Filter Definition tab and under **Foreign Collection** select the Collection target.

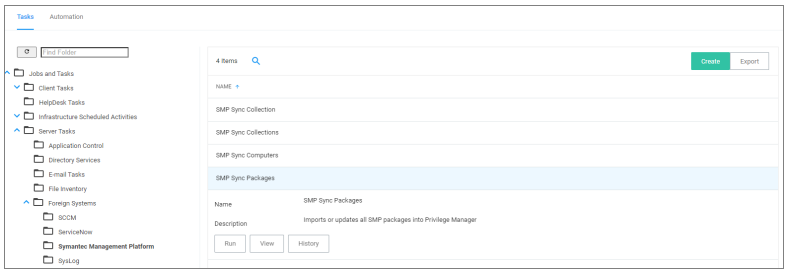


7. Click **Save Changes**.
8. Click the **Sync Foreign Collection** to update the membership immediately. The foreign collection update can also be scheduled by following the link in the help tip.
9. Select the Membership tab and then click the **Update Membership** tab to see the current membership of this collection.

Inventory Software Packages

Once the Foreign System has been created, an on-demand packages synchronization can be run and/or a regular synchronization schedule can be set-up via the following steps:

1. Navigate to **Admin | Tasks**.
2. On the Tasks tab open the folder tree and select **Server Tasks | Foreign Systems | Symantec Management Platform**.
3. Click **SMP Sync Packages**.



4. Click **Run**.
5. Select your SMP system via the **Select...** option.

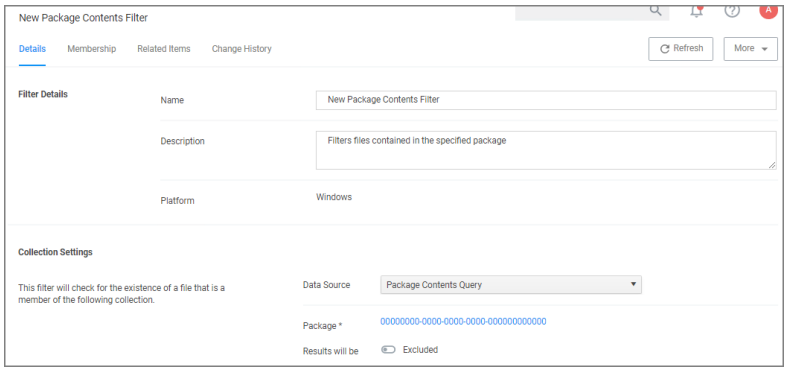
6. Click **Run Task**.

Alternatively the **SMP Sync Packages** task can be scheduled to regularly repeat. When viewing the task, navigate to the Schedules tab and create a new schedule.

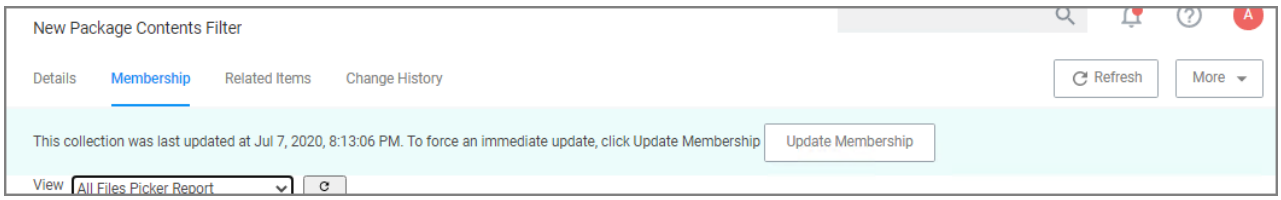
Create a SMP Package Content Filter

After the Package Synchronization completes the SMP Packages can be used in application control policies via package content filters.

1. Navigate to **Admin | Filters**.
2. Click the **Create Filter** button.
3. From the Platform drop-down select **Windows**.
4. From the Filter Type drop-down scroll to Inventory Filters and select the **Package Contents Filter**.
5. Set the Name and Description of the filter.
6. Click **Create**.
7. Next to Package, click **Select resource...**.
8. Select the package from SMP that will be targeted.
9. Set the switch **Results will be** to **Included**.



10. Navigate to the **Membership** tab.
11. If no items are listed in the membership table, click the **Sync Package** button.



Running the sync package task, causes the server to inventory the package referenced in the filter. If you have multiple filters and packages, Delinea recommends to use the *Inventory Packages Referenced in Allow Lists* task instead.

12. Click **Save Changes**.

This filter can then be referenced in Application Control policies.

Simple Mail Transfer Protocol (SMTP)

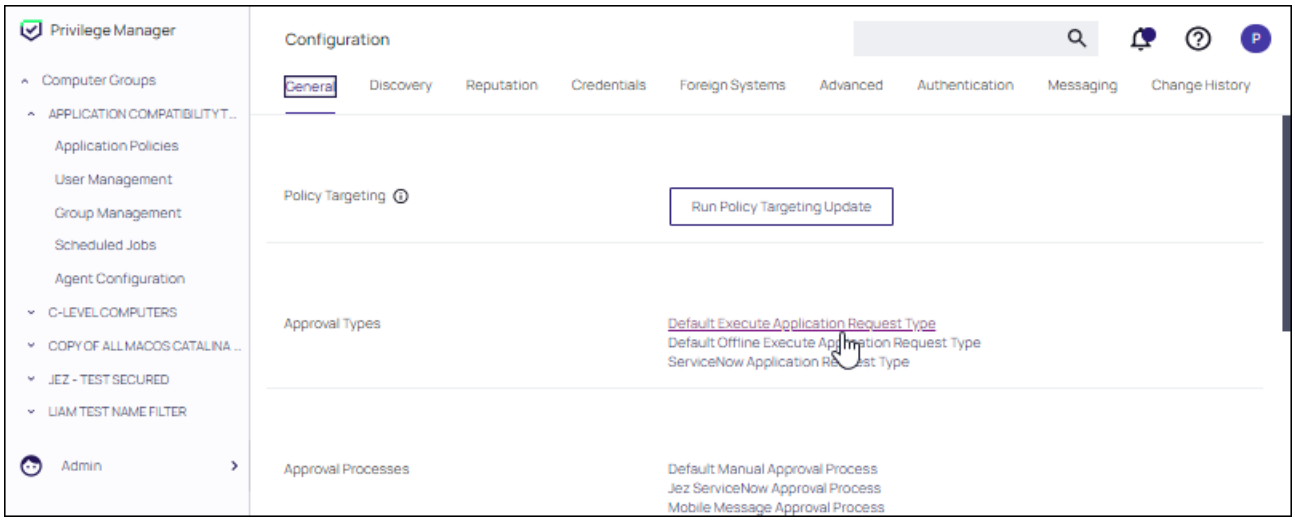
Setting up an SMTP Connection

Simple Mail Transfer Protocol (SMTP) is the Internet standard for email transmission. Often organizations use an SMTP Server – or a server that is specifically dedicated to transmitting email messages via TCP Port 25 – and in order to send email alerts with Privilege Manager policies, you must ensure that your email server is connected to Privilege Manager.

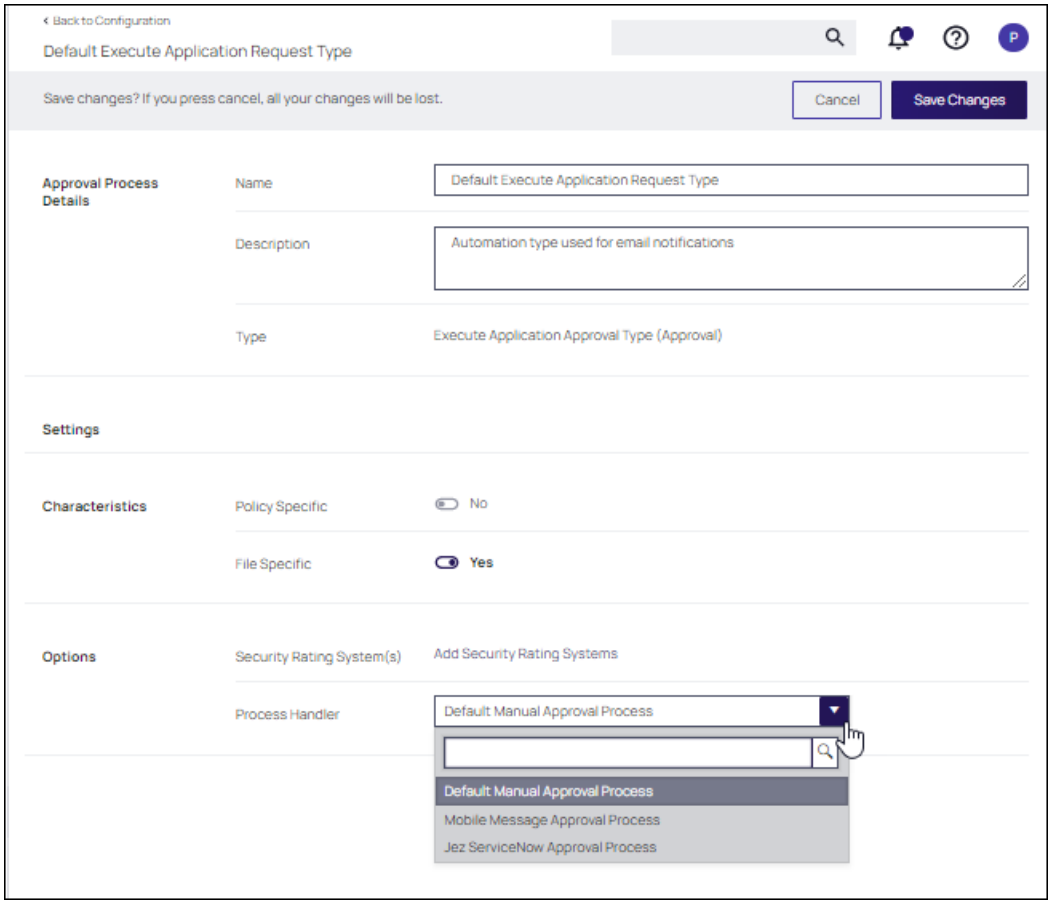
Note: SMTP in Cloud Environments: Starting with version 10.7.1 of Privilege Manager Cloud, the SMTP foreign system is automatically configured with the email server information as provided during the cloud instance set-up. The information can be added/changed following the initial set-up.

To set up the connection, follow these steps:

1. Navigate to **Admin** | **Configuration**.
2. On the **General** tab, select **Default Execute Application Request Type**.



Provide information for the request type at the Default Execute Application Request Type page, then click **Save Changes**.



3. On the **Foreign Systems** tab, click **SMTP Server**, then **Create**.
4. Add the Name of your SMTP Server and the base URL (ex: smtp://[hostname]:[port]), then **Create**.

Next, in order to begin email alert notifications for a policy, you will need to assign a Task for the job. The **Setting Up Email Alerts** information below is just one example of tasks that can be configured for automated email notifications.

Configuring the Email Approval Process Policy

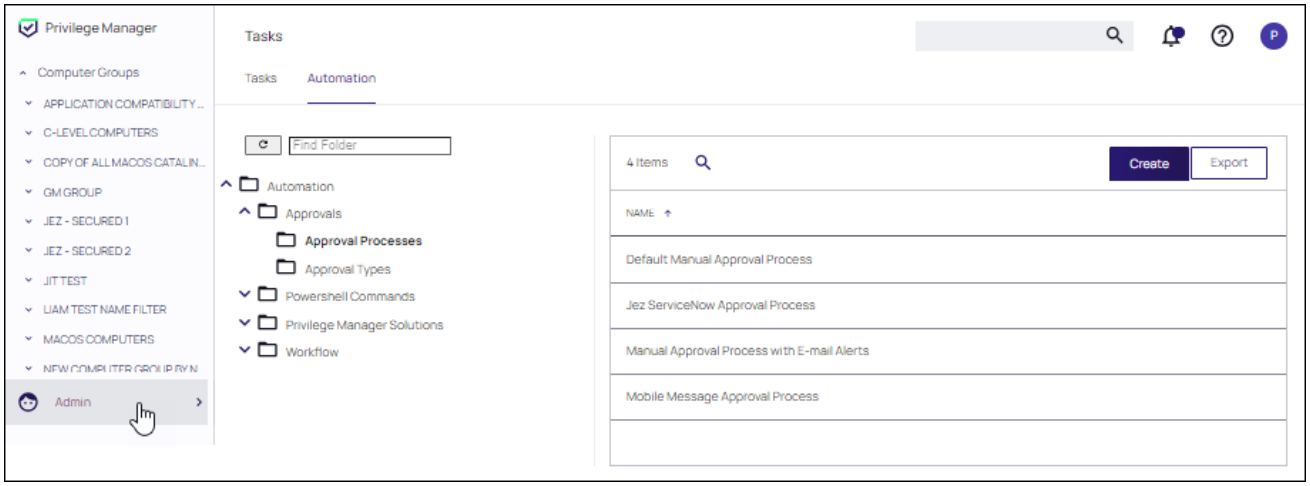
Prerequisites

Prior to creating a new Email Approval Process policy, the following items must be present, or configured if not present:

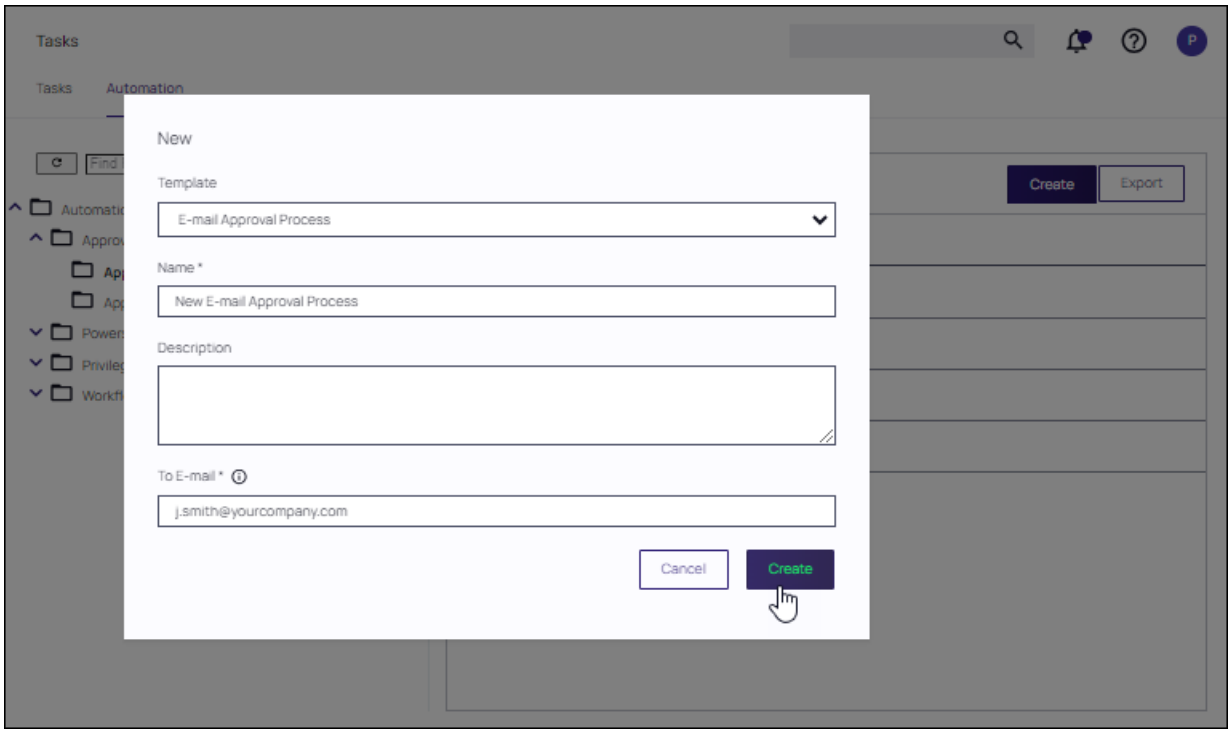
- Approval Process
- Approval Type

Creating an Approval Process

1. From the left navigation panel, select **Admin** | **Tasks** and select the **Automation** tab. In the Automation tree, open **Approvals** | **Approval Processes**. Ensure that you have an Approval Process that can be added to the request form.
2. If an Approval Process is not present, click **Create** .

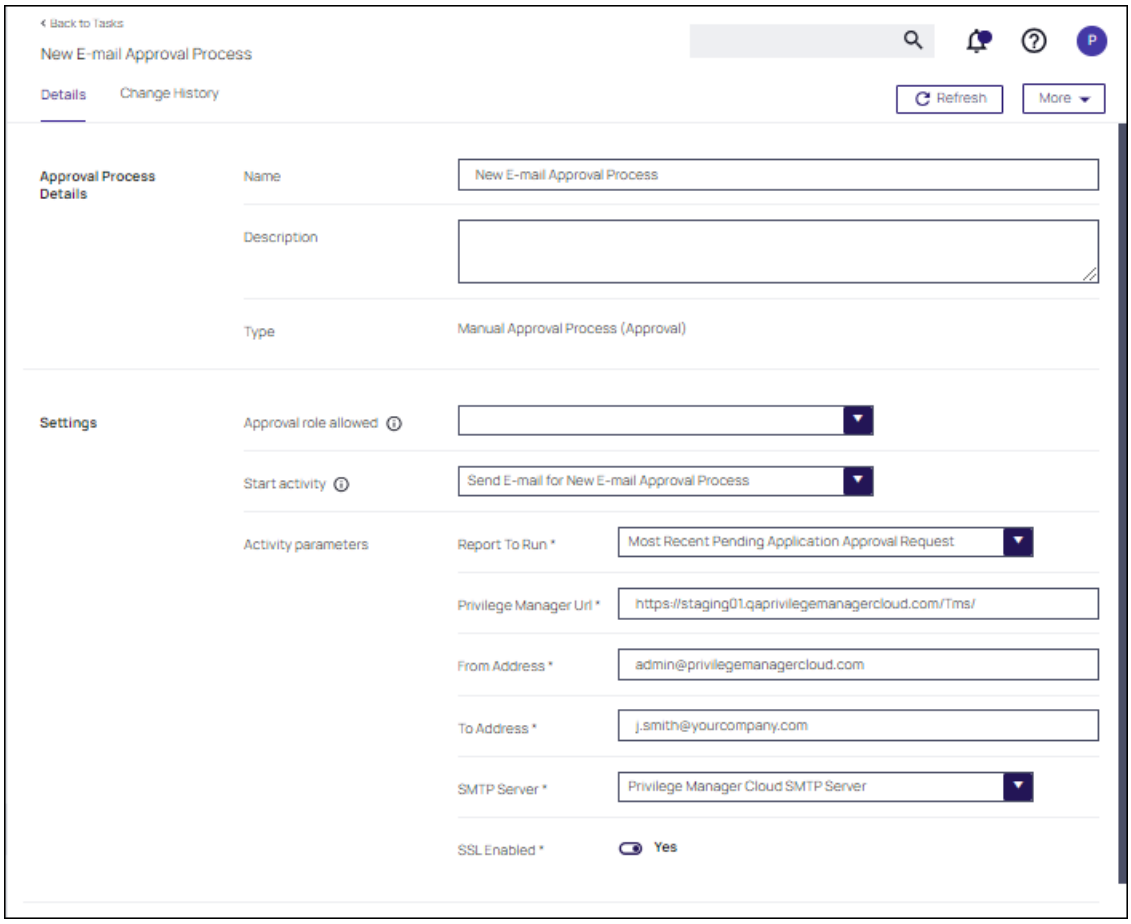


3. Select **E-mail Approval Process** at the Template pull-down.
4. Supply a Template, Name, Description, and Email Address that will receive the email request for approval.
5. Click **Create**.



6. At the new E-mail Approval Process, the only parameter that required editing is the **To Address**. Supply an email that will be notified for approval.
   - Ensure that **Report To Run** is set to **Most Recent Pending Application Approval Request.**
   - **Start activity** should reflect the Approval Process configured.

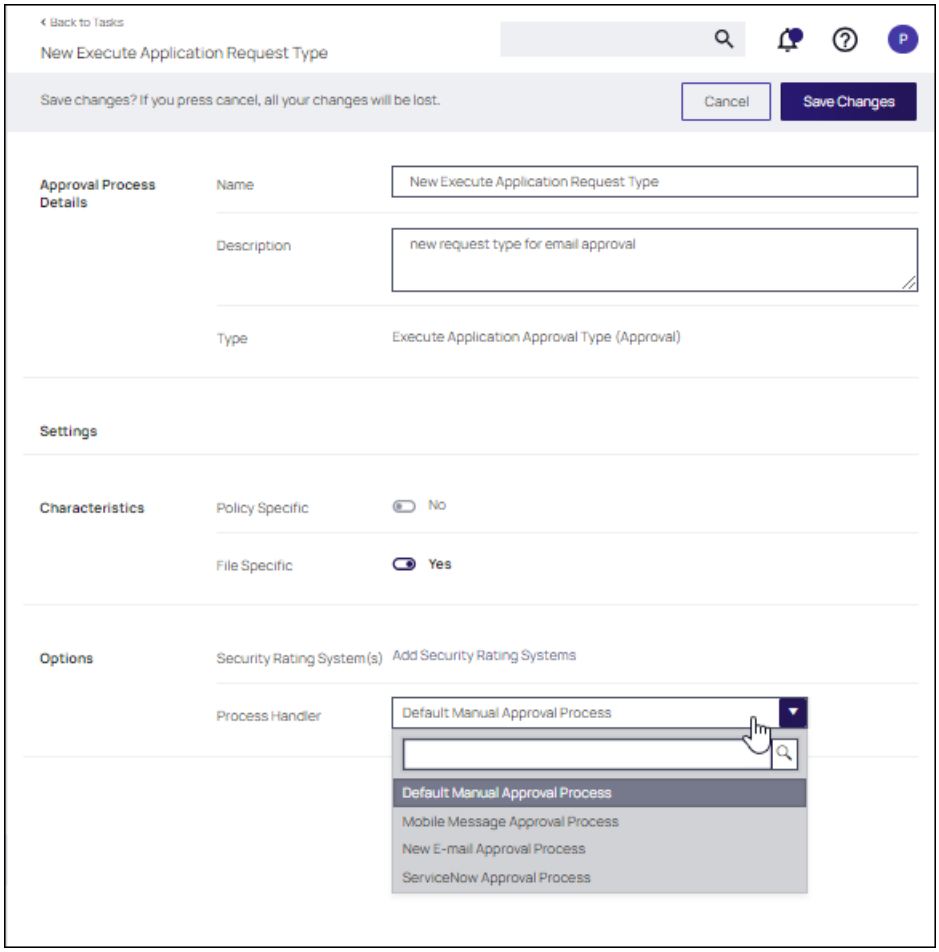
Note: For Privilege Manager cloud, do not edit **From Address**. This has been configured for you. For on-prem applications, this is dependent on your SMTP setup.



Creating an Approval Type

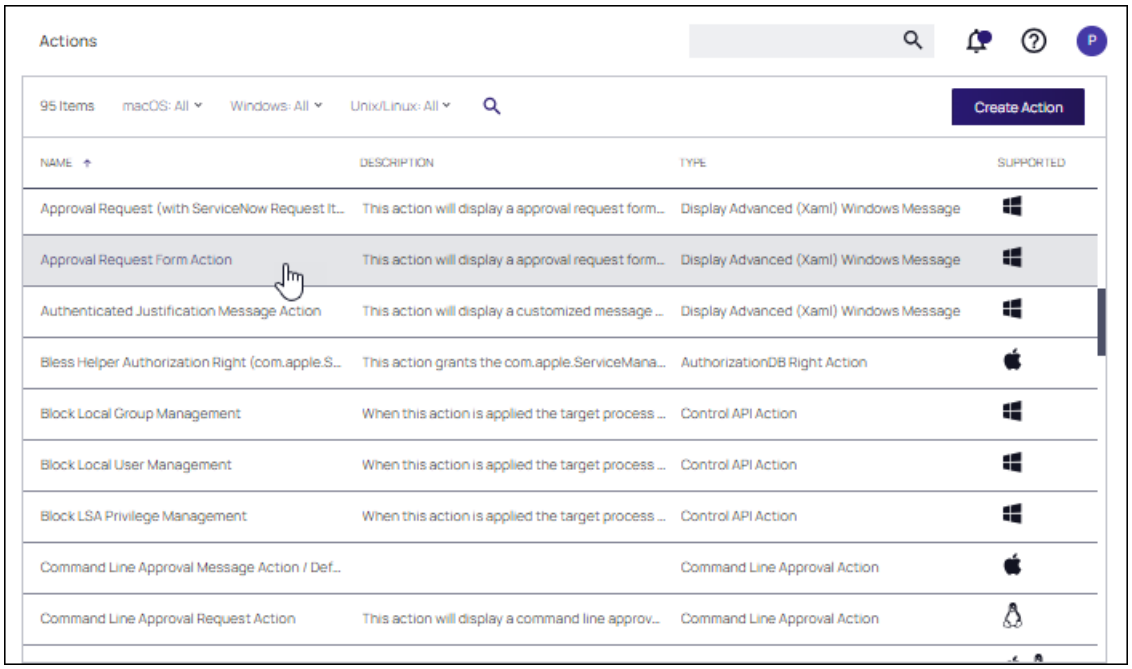
1. From the left navigation panel, select **Admin** | **Tasks** and select the **Automation** tab. In the Automation tree, open **Approvals** | **Approval Types**.
2. Ensure that you have an Approval Type that can be added to the request form. If an Approval is not present, click **Create** .
3. Ensure that the following parameters are set at the Application Request Type:
   - **Options**: Specify the **Process Handle** you created for the Application Request Type.
   - **Characteristics**: Enable **File Specific**.
   - **Process Handler**: Specify the E-mail Approval Process.

4. Click **Create**.



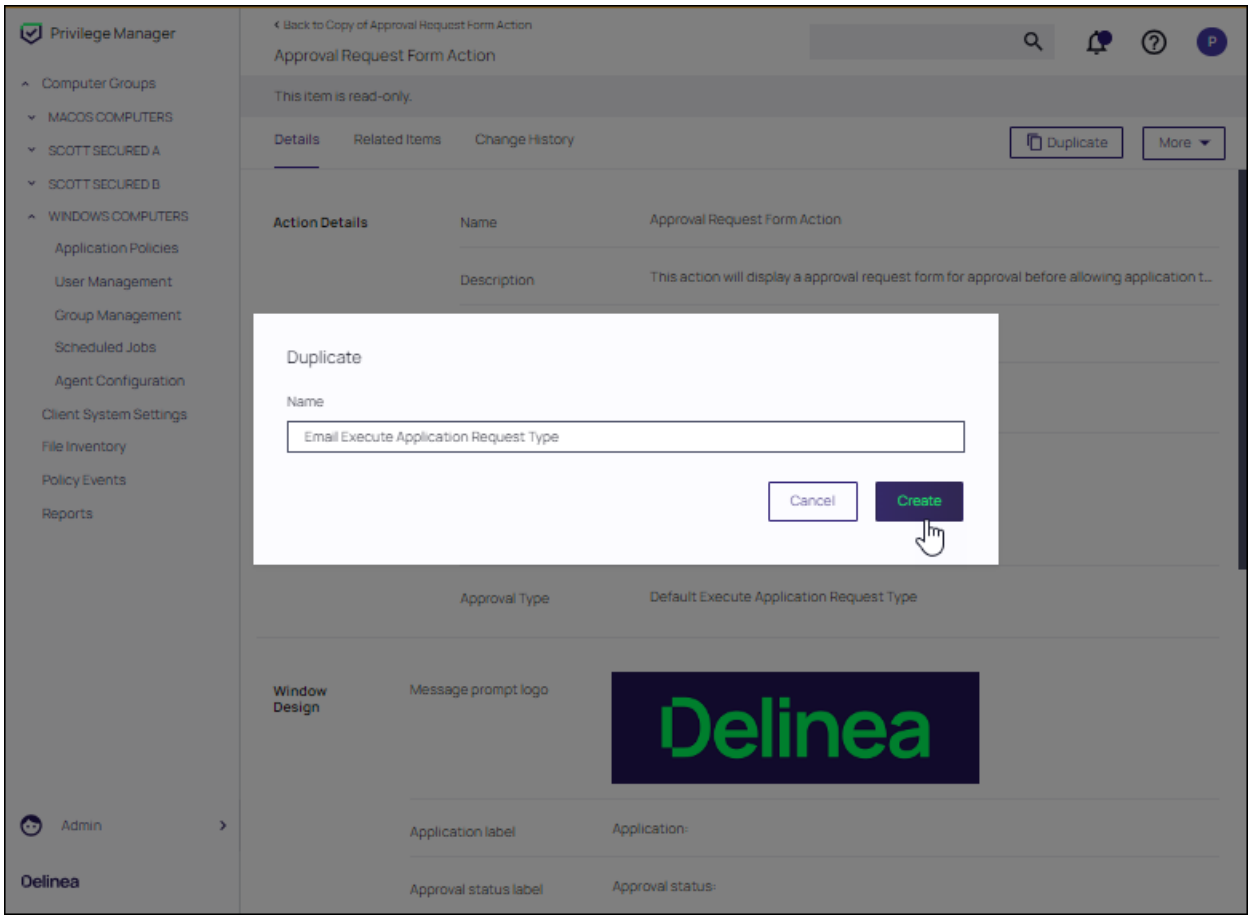
Creating the Application Policy

1. First, locate the Approval Request Form Action that will be used in the policy. Select **Admin** | **Actions** and select the **Approval Request Form Action**.



2. At the Approval Request Form, click **Duplicate** Supply a name for the duplicate form, then click **Create**.

   Delinearecommends renaming the Approval Request Form Action something specific and recognizable. For example, "Email Approval Request Form Action." The **Approval Type** should reflect the Approval Type configured previously. In this example, **Email Execute Application Request Type**.



3. Navigate to the Application Policies for your computer group. Select the Application Policy that will be configured for the process. If one does not exist click **Create** and refer to "Creating Policies" on page 241.

   In this example, the User Access Control (UAC) Override Policy Approval by Email is selected.

   In the **Actions** field, add the **Email Approval Request Form Action**.

   Click **Save Changes**.

Setting up a SysLog Connection

Privilege Manager can push out SysLog formatted messages on a set schedule. Note that this does not happen immediately upon events occurring. Listed below are steps for configuration and task creation for scheduling the action of sending Discovery Event logs to a SysLog server.

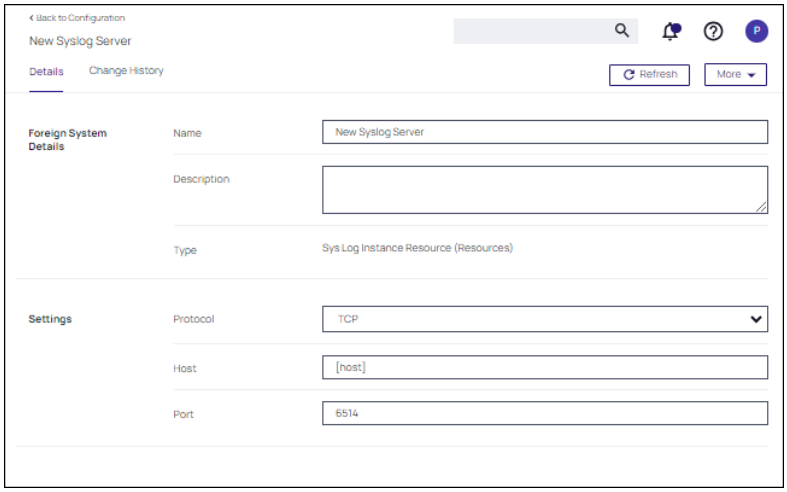
Note: Splunk Cloud doesn't support input directly from Privilege Manager. Refer to the Splunk documentation and reach out to Splunk support as needed.

Configuring SysLog Connection

Note: The Send policy feedback option needs to be enabled on all policies that are supposed to send SysLog formatted events.

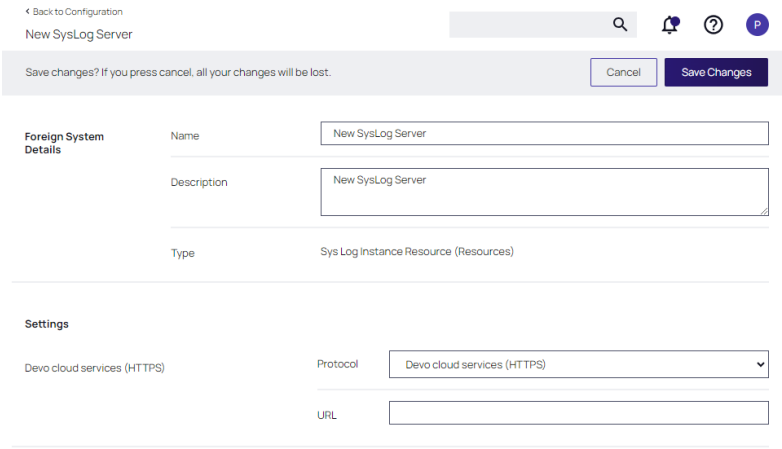
To configure SysLog messages in Privilege Manager:

1. Navigate to **Admin | Configuration** and select the Foreign Systems tab.
2. At the SysLog page, click **Create**. Select a template for the messages, provide a Name and the SysLog Server Address (either tcp or udp). The default is udp on port 514.
3. Once the server is created, you can use **Edit** to change any of the configuration settings.



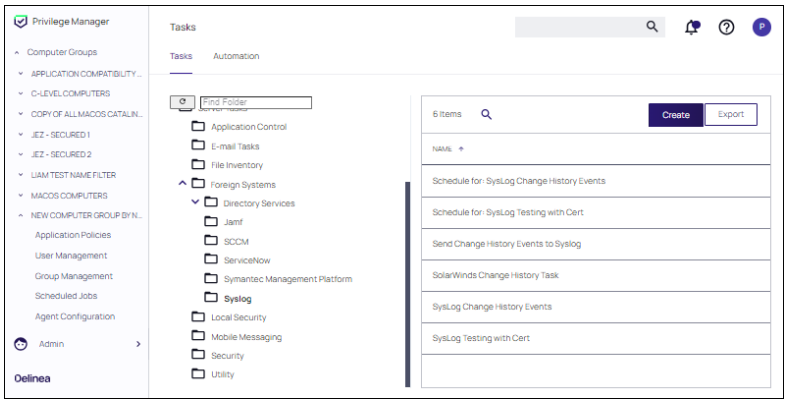
The protocol drop-down options are UDP, TCP, and Devo Cloud Services (HTTPS).

4. Select a protocol and supply the requested parameters, then click Save Changes. (In this example, the Devo cloud services (HTTPS) protocol is selected, and the URL of your Devo cloud instance should be supplied.)

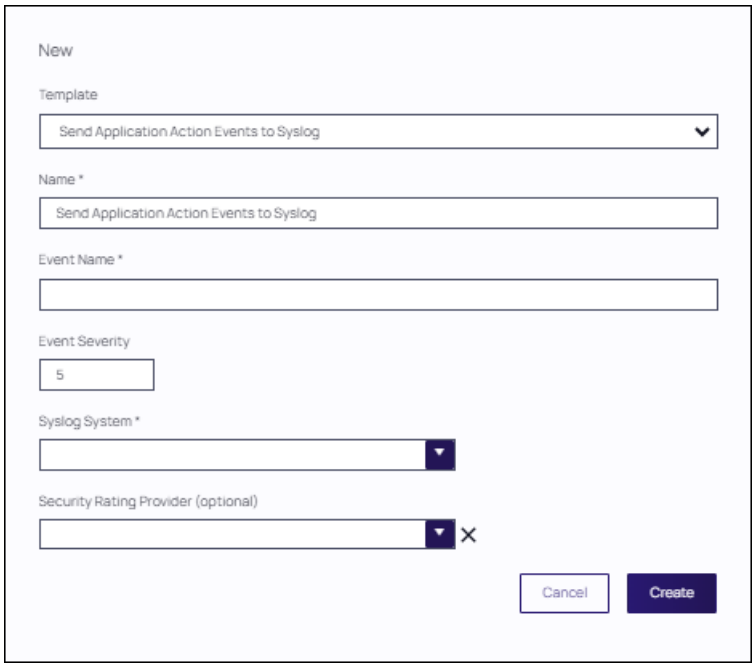


Setting up SysLog Server Tasks

1. After adding a new Syslog connection, to manually send logs to your Syslog Server go to **Admin | Tasks**.
2. Expand the **Server Tasks** folder, then **Foreign Systems**, select SysLog and click **Create**.



3. From the **Template** drop-down, for example select **Send SysLog Application Events**.
4. Add a Name for this task, an Event Name (e.g. “Privilege Manager Application Events”), and Event Severity.
5. From the *SysLog System* drop-down select your SysLog server foreign system (configured above).
6. Optionally also enter a **Security Ratings Provider**, depending on your other integrations. Use the "X" next to the pull-down to remove a selection.



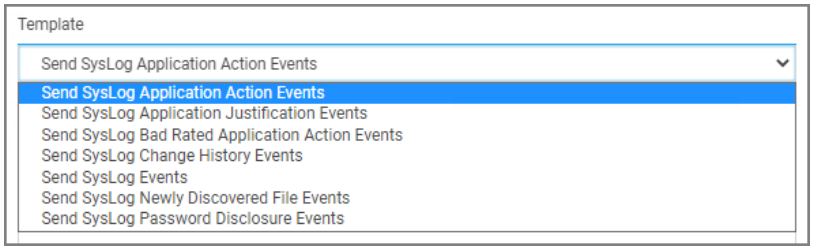
7. Click **Create**.

Once created, you'll be taken to the new Scheduled Task's page where you can run the task on demand and/or specify how often you want events received by Privilege Manager (i.e., all events viewed in **Admin | Event Discovery**) to be pushed out to the SysLog server. The schedule can be hourly, every 30 minutes, daily, or whatever time period is preferred.

After this task runs and successfully completes, verify that Event Discovery events appear in your SysLog system.

Template Options

The following template options are available:



- **Send SysLog Application Action Events** - Use this template to send application action events to your SysLog system. Application Action Events contain generic information about the application that run, which policy was triggered, the date/time stamp, computer, and user for example.
- **Send SysLog Application Justification Events** - Use this template to send application justification events to your SysLog system. For example, if a user runs an application requiring a justification workflow.
- **Send SysLog Bad Rated Application Action Events** - Use this template to send an event to your SysLog system, when an application is being installed or executed, that is identified with a bad security rating.
- **Send SysLog Change History Events** - Use this template to send change history events to your SysLog system. When this task runs for the first time, it sends all change history to your SysLog server. On subsequent runs it only sends the delta of new change history events.
- **Send SysLog Events** - Use this template to send all SysLog events to your SysLog system. These events are based on the different options you selected on the SysLog server during setup.
- **Send SysLog Newly Discovered File Events** - Use this template to send newly discovered file events to your SysLog system. For this to produce any events the Default File Inventory Policy needs to be enabled and resource discovery schedules need to be customized.
- **Send SysLog Password Disclosure Events** - Use this template to send all password disclosure events to your SysLog system.

Data Sources

The following five data sources can be used with the respective templates above:

- **Application Control Justification Events** (7d6bdbf0-8f2a-4e9c-9c7e-fa6b75803c45)
- **Application Control Policy Feedback** (eeb7aaf6-f675-4586-a7e3-3eb54b59ba4d)
- **Recently Discovered Applications Query** (b875d3a6-433c-42cc-8332-05350343e498)
- **Local Security Password Disclosure Events** (13d6cf4d-0132-4401-88ab-80b55301c60c)
- **Application Control Policy Feedback Restricted to Security Level** (4eb4ec69-d7a9-4797-972a-41855d3e7799)

If custom data sources are used, they need to specify the following fields:

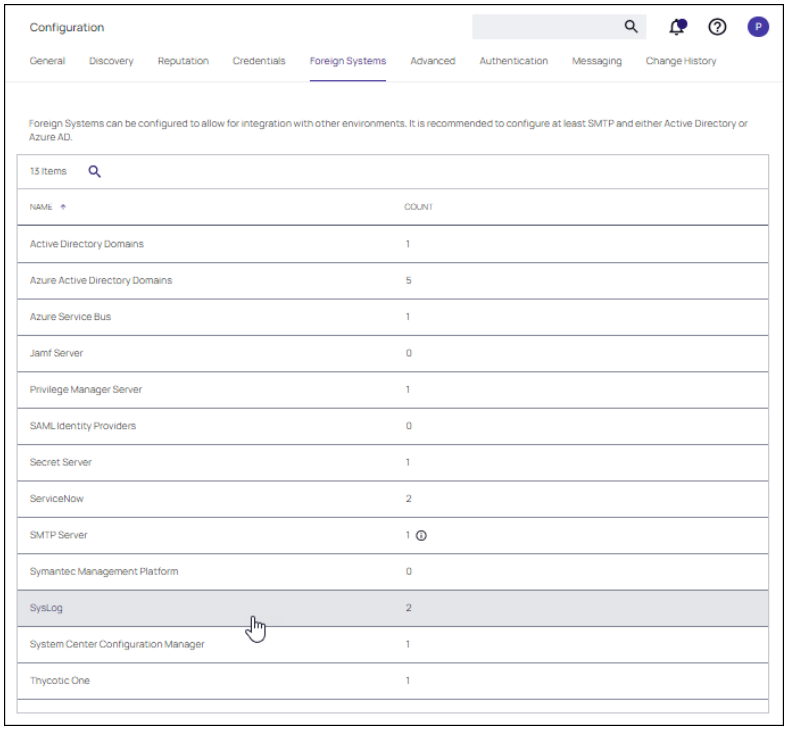
- externalId
- Facility
- Severity
- EventTime
- Host
- DeviceVendor
- DeviceProduct
- DeviceVersion
- Name
- CEFSeverity

Client Certificate Authentication

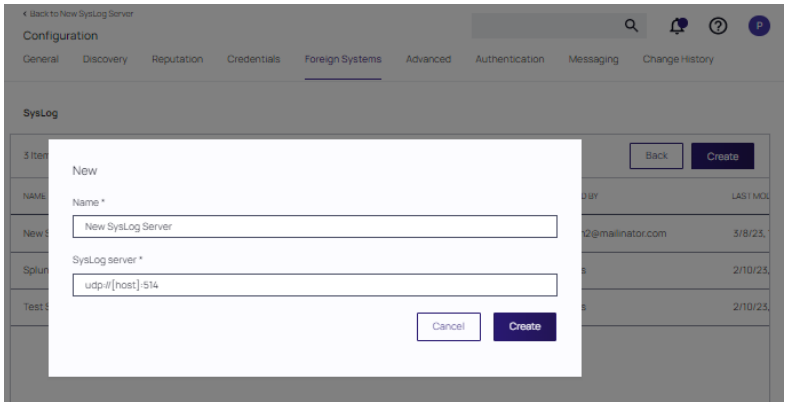
In order to prevent unauthorized systems from sending data to a syslog/SEIM system, users can now use client certificate authentication. In the configuration of a syslog system the **Certificate** field allows you to upload a certificate .pfx file. The option is only relevant if you select TCP + TLS. Once configured Privilege Manager will use this certificate to authenticate all connections when sending syslog events.

Note: A .pfx file must be used since the private key is required.

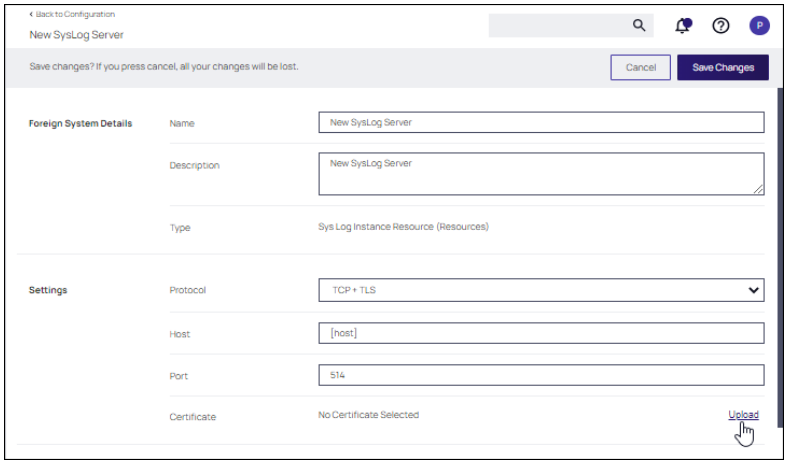
1. Select **Admin** | **Foreign Systems**.
2. On the Configuration page, select the **Foreign Systems** tab. Then, click **SysLog**.



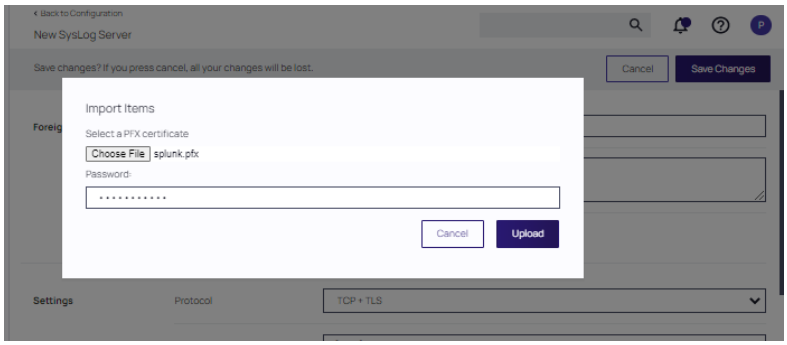
3. Click **Create**. Then, supply a **Name** and address of the **SysLog server**. Click **Create**.



4. On the New SysLog Server page, select **TCP + TLS** for protocol.
5. Click the **Upload** link.



6. At the Import items form, click **Choose file**, browse to the .pfx file and click **Upload**.



The certificate appears in the **Certificte** field. A **Remove** link is available if needed.

Troubleshooting if SysLog Option is Missing under Foreign Systems

If you are a Privilege Manager Cloud customer, contact Delinea support to have it added to your instance.

On-premises customers, navigate to https://[YourOrganizationURL]/TMS/Setup/ProductOptions/SelectProducts and check the Delinea SysLog Connector option. Install the SysLog Connector and accept the License Terms and Conditions.

Setting up a VirusTotal Connection

Privilege Manager can perform real-time reputation checks for any unknown applications by integrating with analysis tools like VirusTotal. This article shows how to set up the integration between Privilege Manager and VirusTotal and then create a monitoring policy in Privilege Manager for reputation checking.

VirusTotal API Key

As a first step the VirusTotal Ratings Provider has to be configured. For this,

1. Sign up for a Free VirusTotal account at https://www.virustotal.com/.
2. Sign in to VirusTotal and find your API key under your **Username | Settings | API Key**.

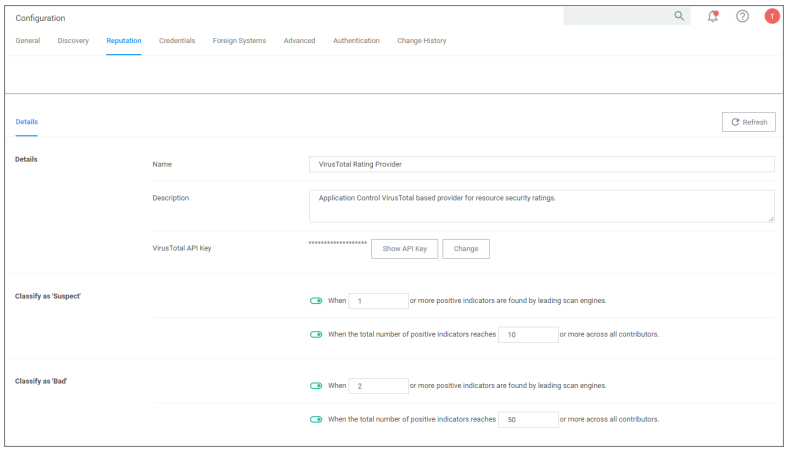
Install VirusTotal

As a second step VirusTotal needs to be installed in Privilege Manager.

Note: You need outbound access on your server for that installation.

1. Open a browser on your Privilege Manager Web Server.
2. Browse to https://YourInstanceName/TMS/Setup/.
3. On the Currently Installed Products screen, choose Install/Upgrade Products.
4. Check the Delinea VirusTotal Reputation Connector, click **Install**. Then **Accept** the End User License Agreement. You will see your Installation Progress.

   Note: If the installation of VirusTotal initially fails, redirect to https://YourInstanceName/TMS/Setup/ and click the **Repair** button next to the VirusTotal Product.
5. Navigate to **Thycotic Privilege Manager | Admin | Configuration | Reputation** tab.
6. Select **VirusTotal Rating Provider** from the Select Rating Provider drop down menu.



7. Enter the **VirusTotal API Key**, click **Update**.
8. Enter information under Details and specify settings for Suspect and Bad classifications.
9. Click **Save Changes**.

> **Note:** VirusTotal can be used without API Key. If the free version is used, reputation checks are limited to 4 per Minute. Delinea does not recommend this for a production environment.

For the implementation example below, we are creating two filters, using one default filter, and creating a policy. One filter is the standard Security Rating Filter the other filter controls, that we only send applications to VirusTotal for a reputation check that are in the user's Downloads and Temp directories.

Further details about creating a Security Rating Filter and other needed filters to work with reputation checking policies refer to the "Reputation Checking" on page 319 topic.

Jamf Integration

Jamf, a software company that specializes in enterprise management solutions for Apple products, allows IT administrators to enforce policies, perform remote wipes, and disable services, for example, securely, efficiently, and seamlessly.

Privilege Manger integrates with Jamf Pro to allow users to:

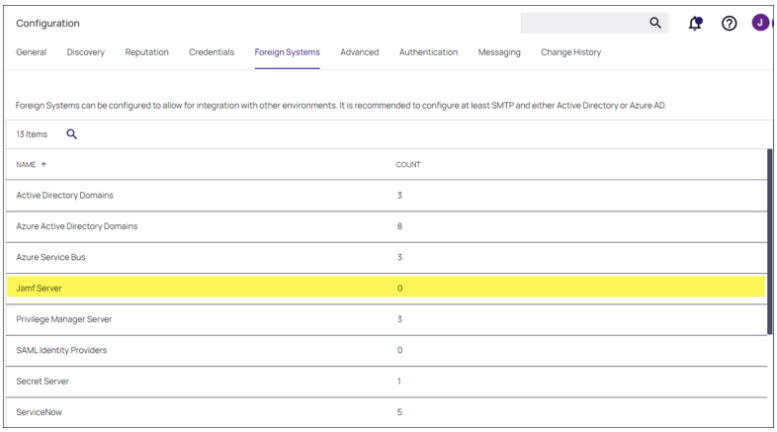
- Import Smart Computer Groups and Static Computer Groups
- Import installed applications on Jamf endpoints, leveraging resources and filters.

Connecting to the Jamf Server

Before you can import data from Jamf Pro, you need to setup a foreign systems connection in Privilege Manager for the Jamf integration.

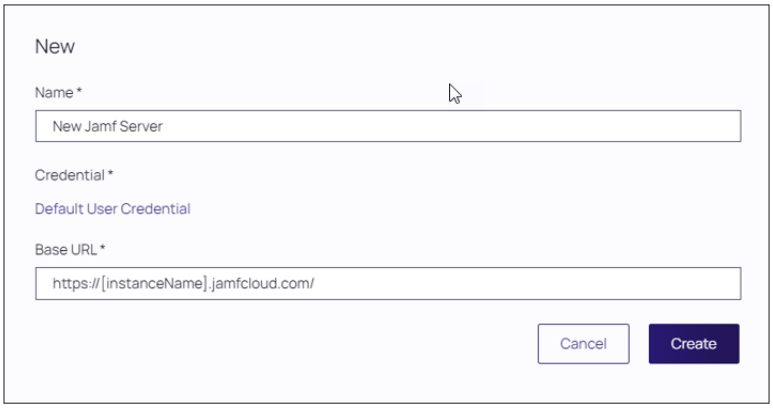
1. Navigate to **Admin** | **Configuration** | **Foreign Systems**.
2. Select **Jamf server**. If this is not listed, make sure the connector is installed. Refer to Installing Foreign System Connectors.

Note: If you are a cloud customer and don't see Jamf in the list, contact Delinea support to have the connector added to your cloud instance. Once it is listed, continue with the next step.

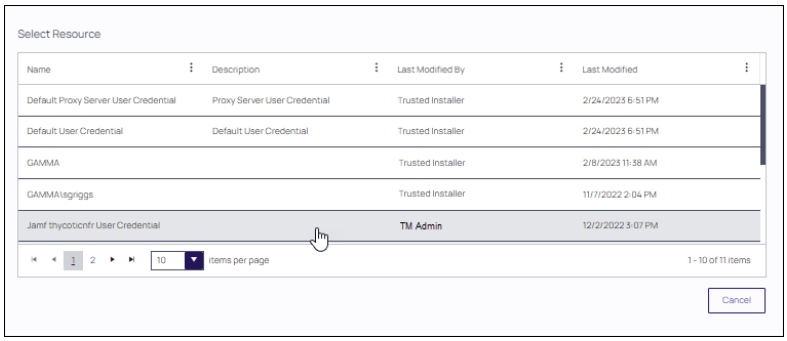


3. Click **Create** to establish a Jamf server.
4. From the **New** window, enter the **Name** of your **Jamf Server**.
5. Click **Default User Credential**.

Note: The Privilege Manager Default User Credential is populated by default and needs to be changed to the actual Jamf credential.



6. From the **Select Resources** dialog, select the credential you established. Click **Select**.



7. The **New** dialog is returned with your selection in the **Credential** field. Enter the **Base URL** of your Jamf Server.
8. Click **Create**.

Creating a Privilege Manager Credential

Privilege Manager needs a username and password to access Jamf PRO. Starting with 12.0, Privilege Manager supports the Jamf Bearer Token Authentication method. This require updating the Privilege Manager credential that is used to connect to Jamf Pro. Refer to the Prerequisites.

Prerequisites

From your Jamf Pro Instance, create an API role and API client that will be used by Privilege Manager to connect to your Jamf instance.

This is done in your Jamf Pro Cloud Server, under Settings | API roles and clients and requires:

- An API role that contains the following Privileges: Read Smart Computer Groups, Read Computers, Read Static Computer Groups.
- An API client that is assigned the role you just created.

Important: Make sure to note the Client ID and Client Secret, as these will be required to create your user credential in Privilege Manager.

Creating the Credential

Privilege Manager needs a username and password based on the API Client created to access Jamf PRO. To create the credential in the Privilege Manager:

1. Navigate to **Admin** | **Configuration** | **Credentials**.
2. Click **Create**.
3. Enter a **Name** in the **Details** section.
4. In the **Settings** section:
   a. Enter Jamf API Client as the **Account Name**.
   b. Enter the Jamf API Client Secret as the **Password**.
5. Click **Save Changes**.

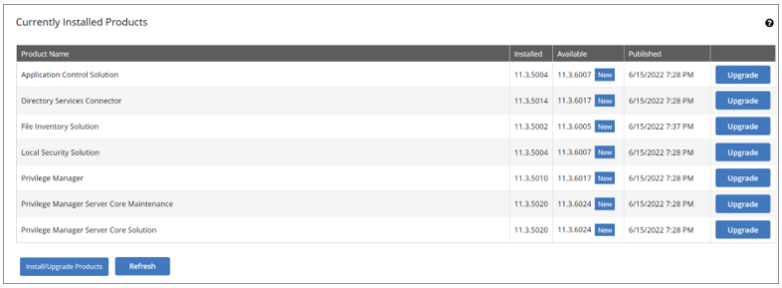
Installing the Jamf Connector

On-Premise Customers

For on-premises Privilege Manager instances, you must install the Jamf Connector before you can configure this solution from the Privilege Manager console. it can be setup in the console. Refer to "Getting Started Overview - On-Premise" on page 93 for a general overview of on-premises setup and rollout recommendations.

For on-premises Jamf installation:

1. Navigate to **Admin** | **Setup**.
2. Click **Install/Upgrade Products**.



3. Select **Jamf Connector** from the product list that appears.
4. Click **Install**. The installation takes approximately 15 minutes to complete.

Cloud Customers

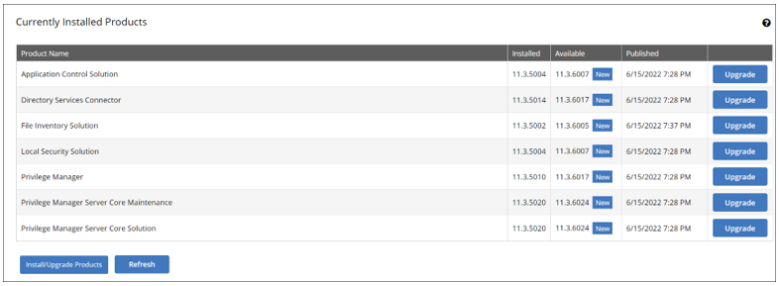
For cloud Privilege Manager instances, you must install the Jamf Connector before you can configure this solution from the Privilege Manager console. Refer to "Initial Setup - Cloud" on page 100 for a general overview of cloud setup and rollout recommendations.

For cloud Jamf installation:

1. Manually navigate to your cloud instance, entering the Privilege Manager URL into the browser.
2. Navigate to **Admin** | **Setup**.

   Note: If the **Setup** option is not available, consult Delinea Support for assistance.

3. Click **Install/Upgrade Products**.



4. Select **Jamf Connector** from the product list that appears.
5. Click **Install**. The installation takes approximately 15 minutes to complete.

Synchronizing Jamf Computer Groups

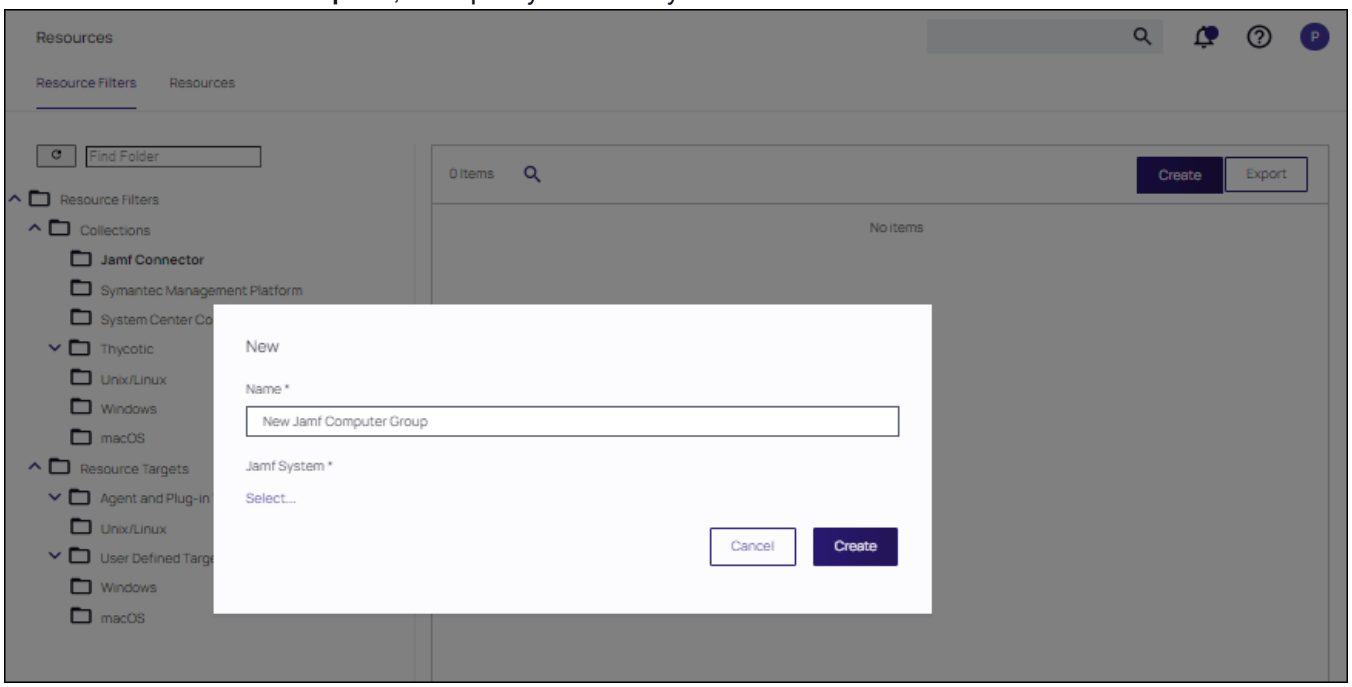
To import computer groups from the Jamf Server, the **Synchronize Jamf Computer Groups** task must run. This task also imports related computer resources.

1. First, create the foreign collections for the sync. Navigate to **Admin** | **Resources** and open the **Resource Filters** tab.

1. In the folder tree under **Resource Filters** open **Collections** | **Jamf Connector**.

1. Click **Create**.

1. Enter a **Name** and **Description**, and specify the Jamf system to connect to.

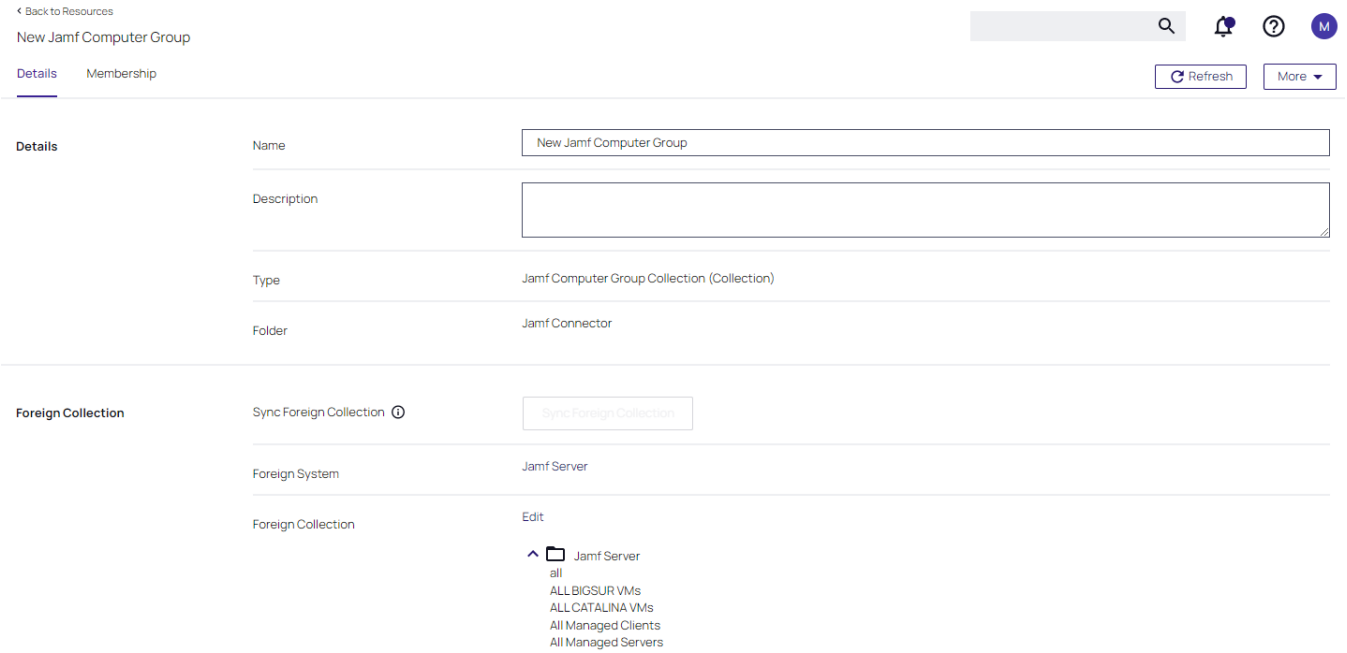


1. Click the **Select** link.

1. At the **Select Resource** dialog, enter a resource name in the **Search text** field. This field can remain blank if you want to search for all available resources. Click **Search** and select a resource.

1. Click **Create**.

1. Next to the **Foreign Collection** field click **Edit** and select the Jamf Computer Group that should be referenced.



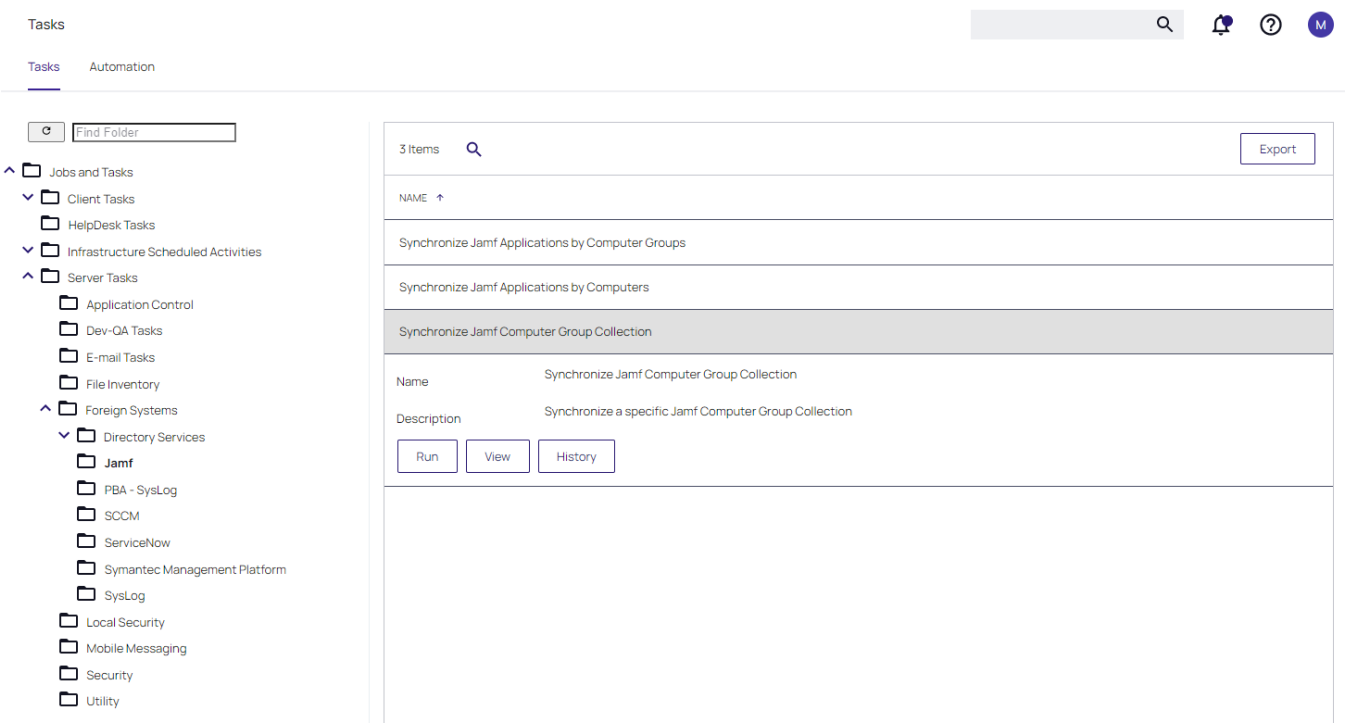
2. Navigate to "Computer Groups" on page 228 and create a new Computer Group that references the Jamf Collection.

3. Navigate to **Admin** | **Tasks**.

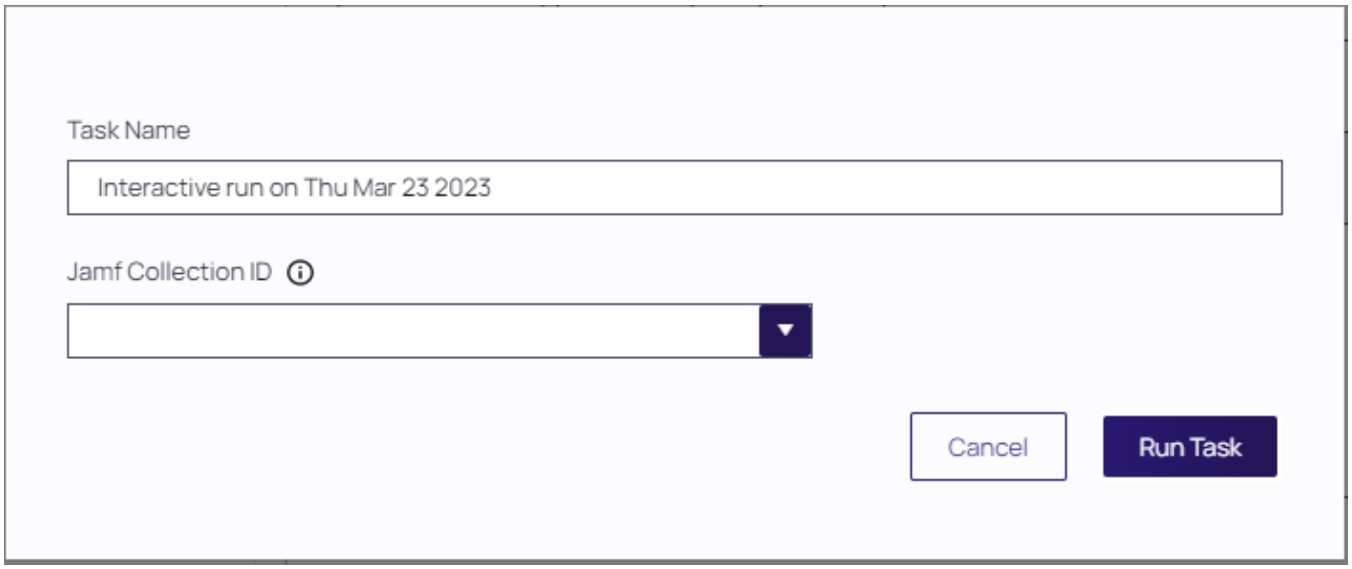
4. On the **Tasks** tab, open the folder tree and select **Server Tasks** | Foreign Systems | **Jamf**.

5. Click **Synchronize Jamf Computer Groups**.

6. Click **Run**.



7. In the **Jamf Collection ID** field, select the collection created in step 4 or leave empty to sync all collections.



8. Click **Run Task**. The task executes and Privilege Manager records the task history.

Privilege Manager returns error codes if tasks fail for the following reasons:

- Jamf connectivity loss
- Invalid credential or URL

Example: Synchronize Jamf Computer Groups

After running the **Synchronize Jamf Computer Groups** task, you can view the results in your "Computer Groups" on page 228.

1. From the Privilege Manager left navigation pane, select **Computer Groups**.

1. Use the scroll bar to navigate the page, expanding the categories as needed. By default, this page displays groups in the Side Menu (or left navigation pane). The drop-down list box indicates **In Side Menu**. To view the computer groups you imported via the Jamf Connector, change **In Side Menu** to **All** or **Not in Side Menu**; otherwise, you might falsely believe the import failed.

Compare Jamf Server with Import

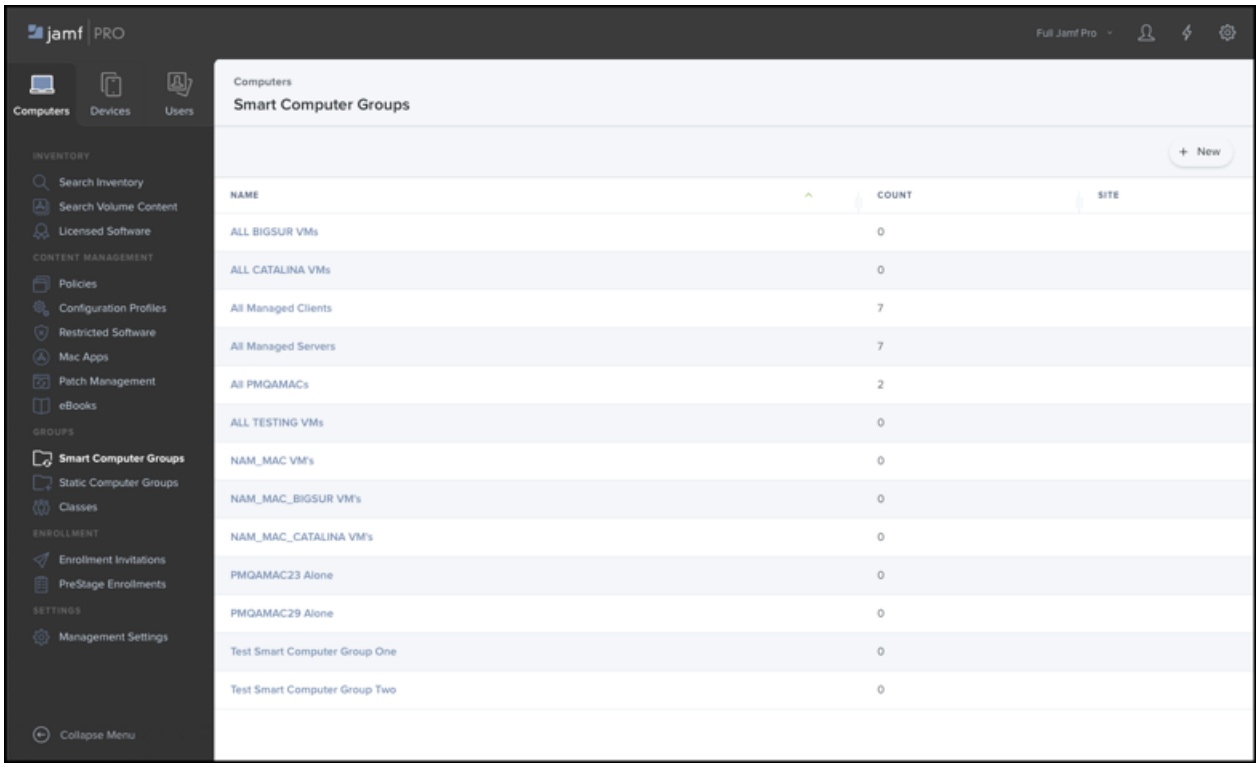
You can compare if the imported Computer Groups correctly reflect the data on your Jamf Server.

1. Access Jamf Pro and enter your login credentials.

1. Select **Computers** | **Smart Computer Groups** or **Computers** | **Static Computer Groups**.

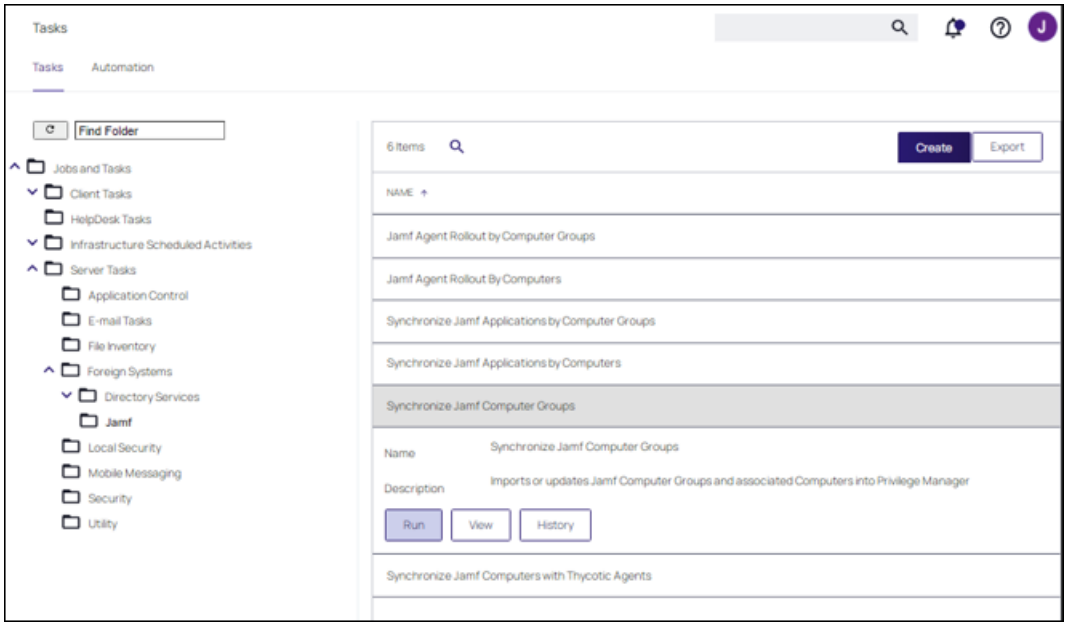
> **Note:** All Computers Groups imported into Privilege Manager contain a static list of computers, derived from a Jamf Pro query.

An **All BIGSUR VMs** group, for example, results from a Jamf Pro query and provides a list of computers that do not originate from Privilege Manager.



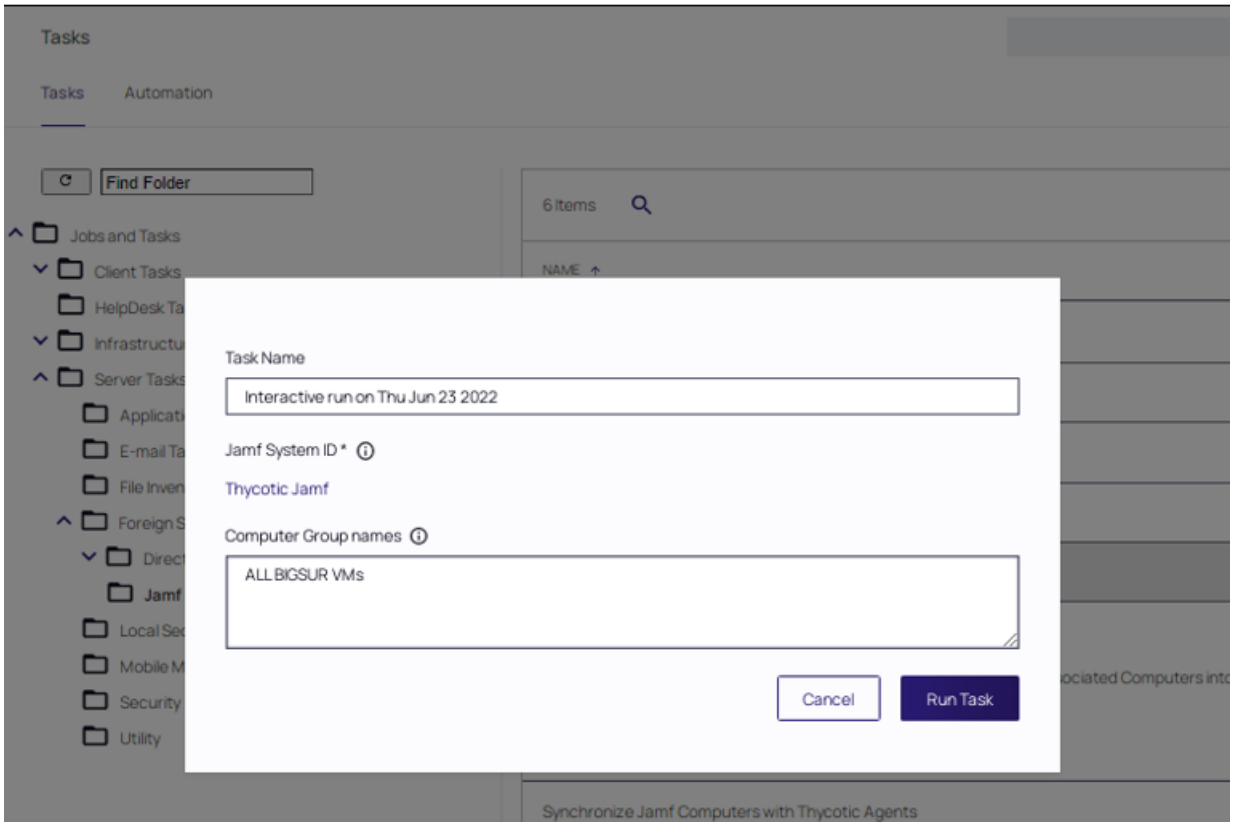
When you import this group into Privilege Manager, the group displays the list of computers that align with the query output above.

1. Run the task.

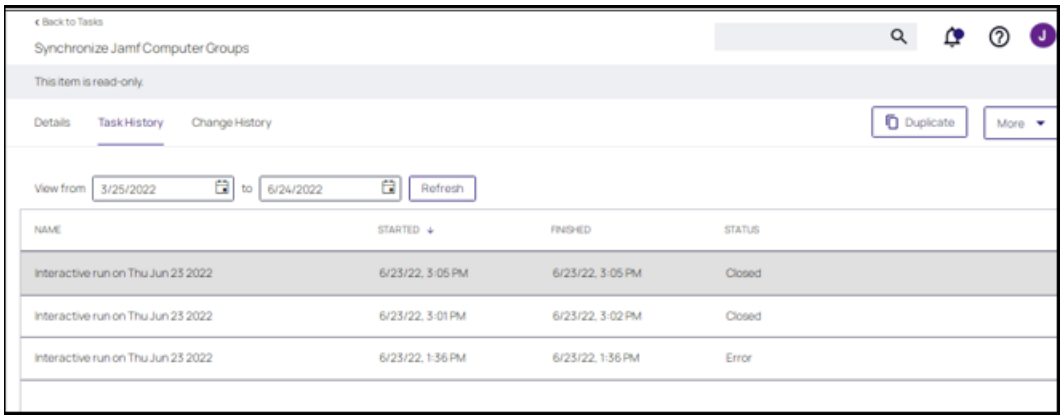


1. Enter the group name.

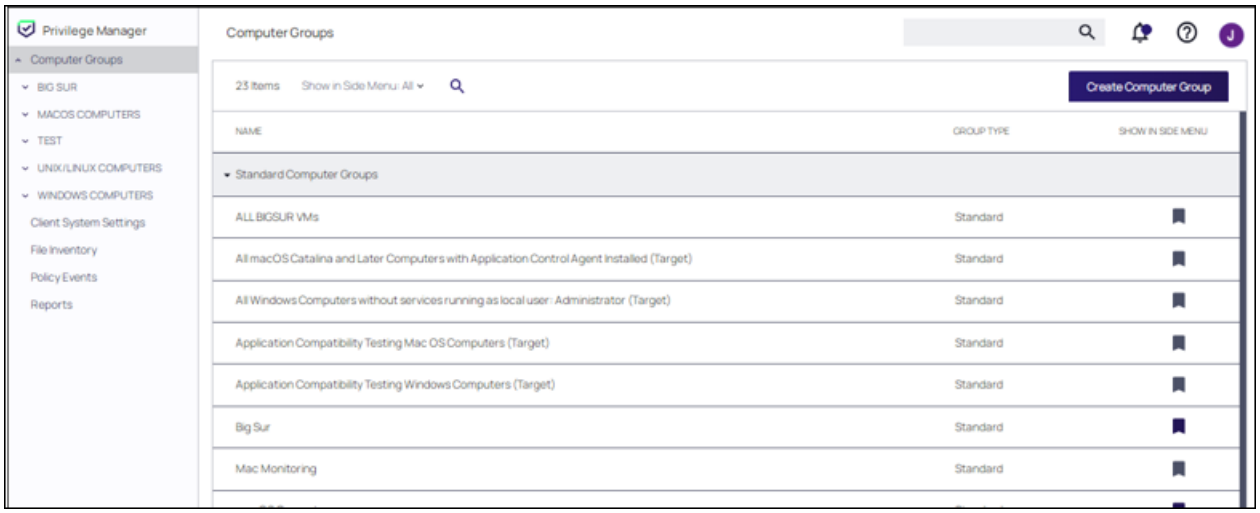
1. Choose your integrated Jamf instance, which populates the **Jamf System ID** field.



The results are visible in **Task History**.



You can also view **ALL BIGSURVMs** under **Computer Groups | All**.



The list updates in Privilege Manager when you run the **Synchronize Jamf Computer Groups** task manually or, alternatively, this list updates automatically when this task executes at a scheduled date/time.

Resources in Privilege Manager

Computers that do not have the Privilege Manager agent installed do not get created from the Jamf Computer Group Sync task.

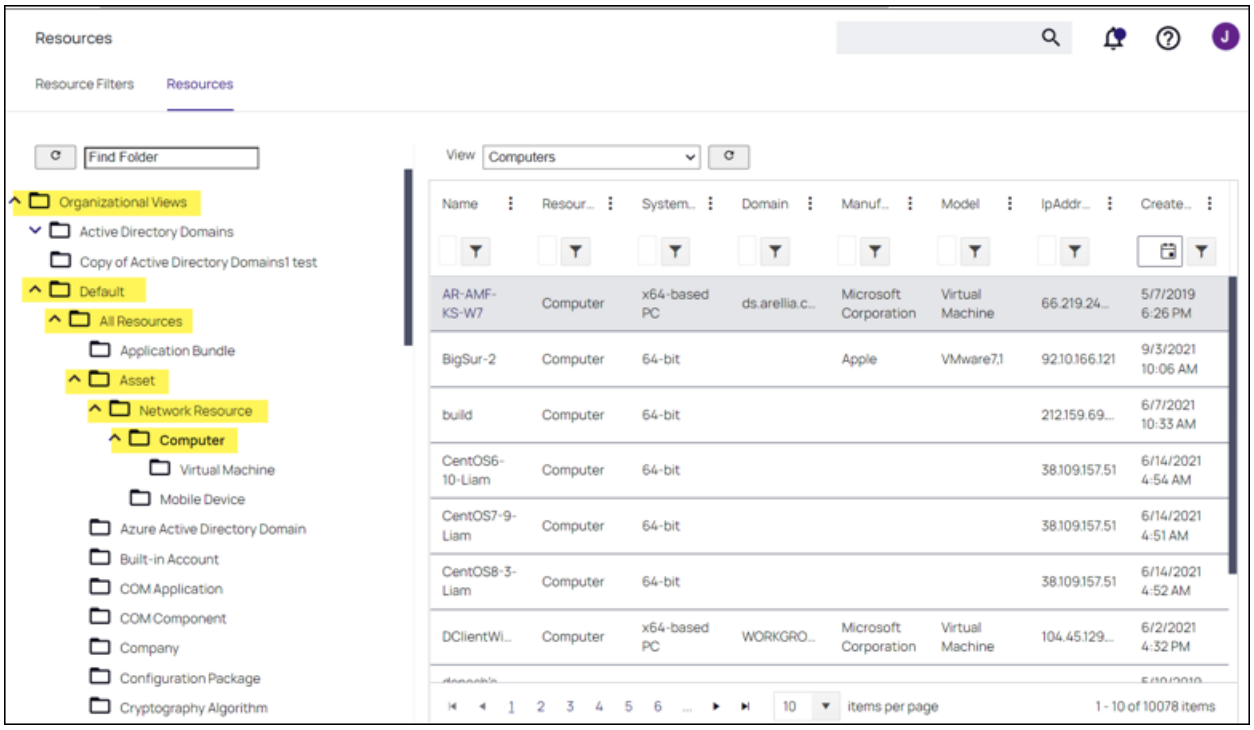
To view existing computer resources in Privilege Manager:

1. Navigate to **Admin** | **Resources**.

1. Select the Resources tab.

1. In the left navigation tree, select **Organizational Views** | **Default** | All Resources | **Asset** | **Network Resource** | **Computer**.

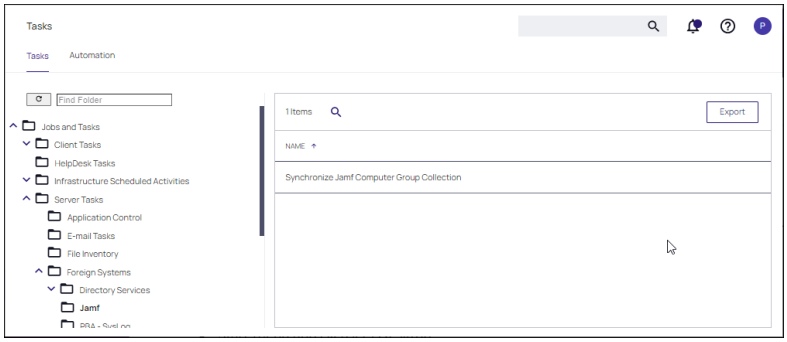
Select any of the synchronized computer resources (**Computer** folder) to view imported inventory details.



Jamf Tasks

These are the tasks created when the Jamf Server is installed.

1. Navigate to **Admin | Tasks**.
2. On the Tasks tab open the folder tree and select **Server Tasks | Foreign Systems | Jamf**. The following task is available:
   - Synchronize Jamf Computer Group Collection



Setting up a SAML Integration

SAML integrations facilitate the authentication and authorization between providers. If required, multiple SAML providers can be created and utilized in a SAML integration.

Note: Currently, Delinea does not support Identity Provider (IDP) initiated connections. Only Service Provider (SP) initiated connections are supported.

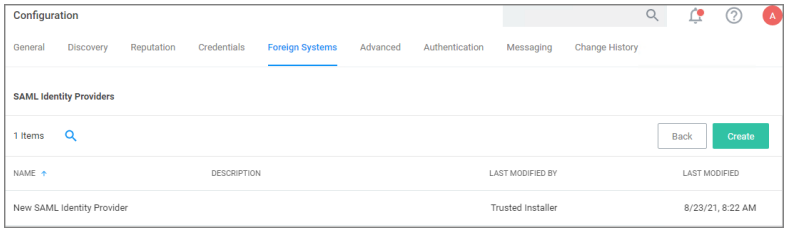
For the purpose of this procedure, we use Okta as the identity provider example. All SAML Foreign Systems integrations follow these same principle steps.

Note: Refer to related Okta topics for nuances associated with Using GSuite as a SAML Provider and Using Privilege Manager Mobile App with Hybrid SSO Logins.

1. Set up the identity provider. Refer to Managing Authentication Providers.
2. Enable authentication for the SAML identity provider on the **Authentication** tab.

Note: Ensure that authentication for the SAML identity provider is enabled or the configuration will fail. Refer to Authentication Tab.

3. Use data from the identity provider setup for setting up the Privilege ManagerForeign Systems.

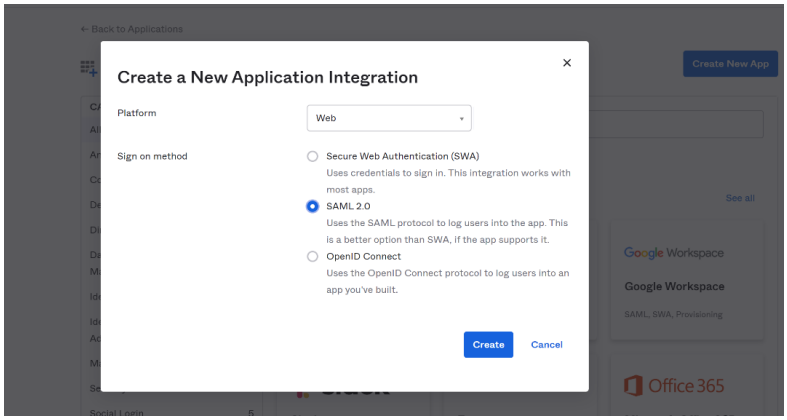


Create a new Application

An application is a definition for integration with an external application (in this case, Privilege Manager).

In Okta, create a new application. Don't select one of the existing:

1. In the top right of the app page, click **Create New App**.
2. From the **Platform** drop-down, select **Web**.
3. From the **Sign on method** options, select **SAML 2.0**.



4. In the **App name** field provide an Application Name. Depending on your use case, provide an application logo and select App visibility settings.
5. Click **Next**.

Enter Application SAML Settings

On the next pages, you'll configure the SAML settings.

1. Enter the **Single sign on URL**. The **Single sign on URL** is the root Privilege Manager URL plus **saml2/acs**. For most systems this is `https://servername/Tms/saml2/acs`.
2. Enter the **Audience URI**, which can be anything as long as it matches what you put in Privilege Manager. The default value in Privilege Manager is `PrivilegeManagerServiceProvider`.
3. The **Default RelayState** can be left blank.
4. The **Name ID format** drop-down set to **Unspecified**.
5. From the **Application username** drop-down, select **Okta username**.

   The rest of the settings can be ignored.
6. Proceed via **Next**.
7. On the last page for the **Are you a customer or partner?** prompt, select **I'm an Okta customer adding an internal app**.
8. Click **Finish**.

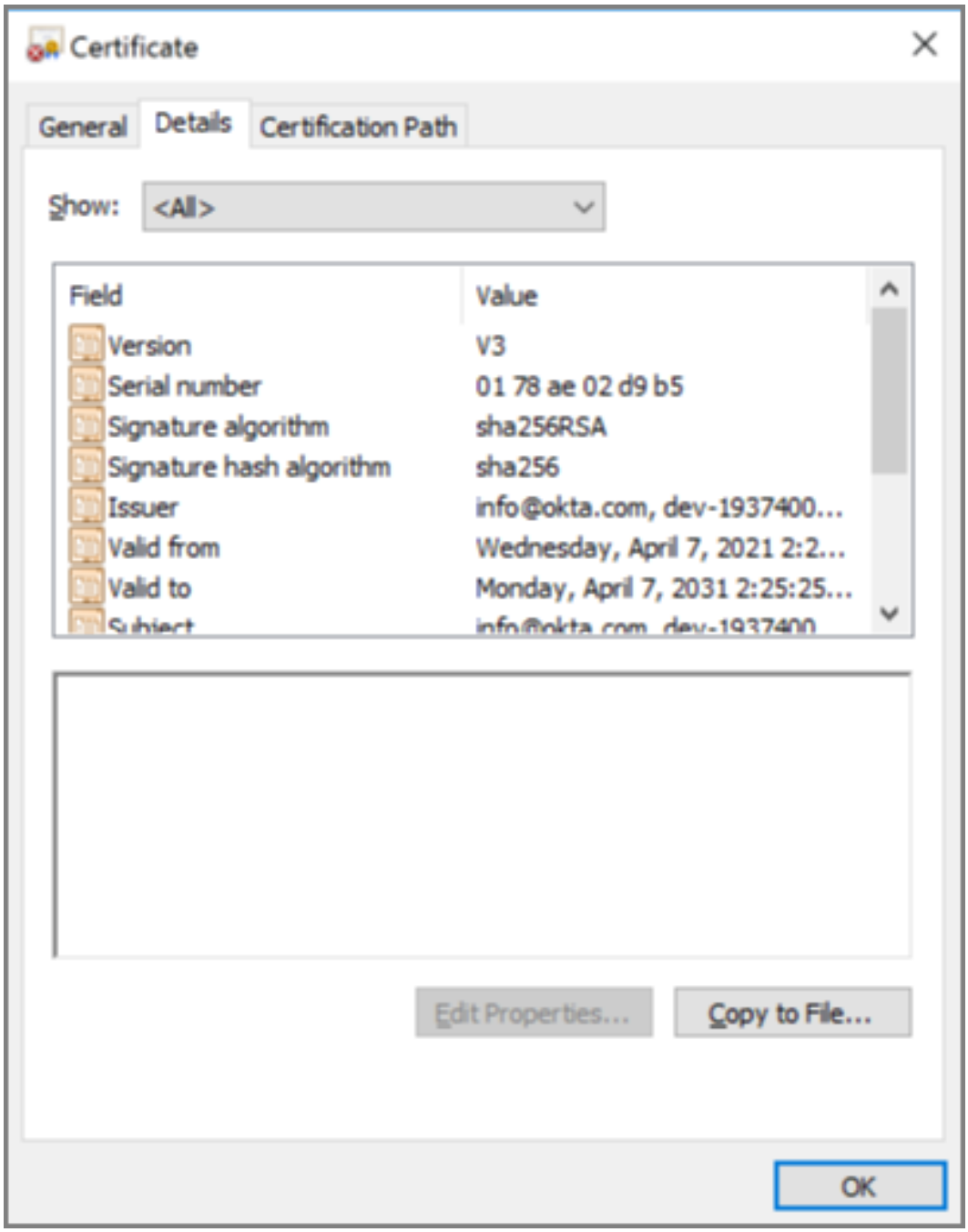
View Setup Instructions

After the app is created, you'll want to click **View Setup Instructions** and leave the instructions open in the browser. You'll want to copy and paste some of this info into Privilege Manager in the next section.

Save Certificate

Start with the certificate data.

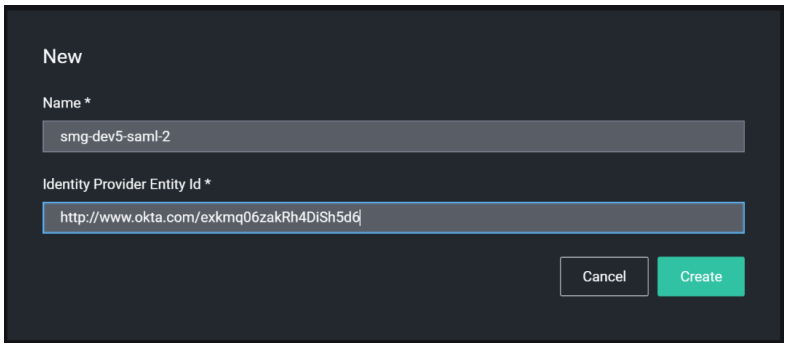
1. Click **Download certificate** and save the certificate as **.cer**. Okta will try to save it as .cert.
2. Once it's saved, you should be able to open and view the certificate in Windows:



Privilege ManagerForeign Systems Setup

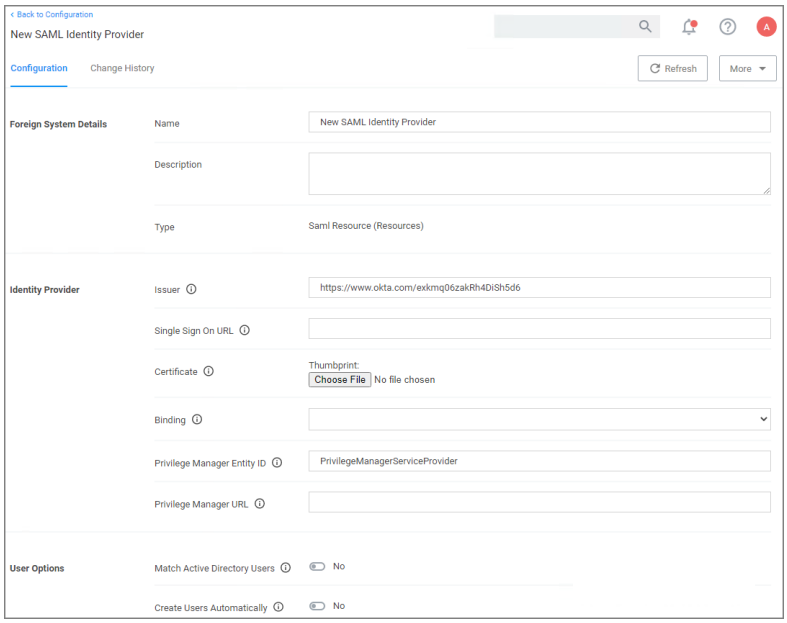
Create SAML Identity Provider

1. Navigate to **Admin | Configuration** and select **Foreign Systems**.
2. Click **SAML Identity Providers**.
3. Click **Create**.

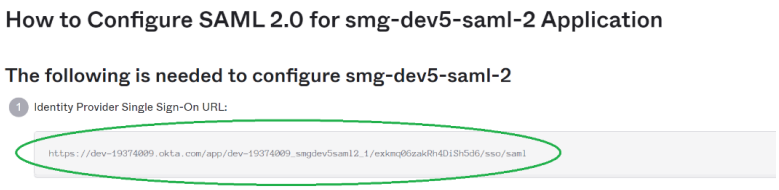


4. Enter a name for the Foreign System.
5. For **Identity Provider Entity Id**, enter the issuer name from the setup instructions. For example:

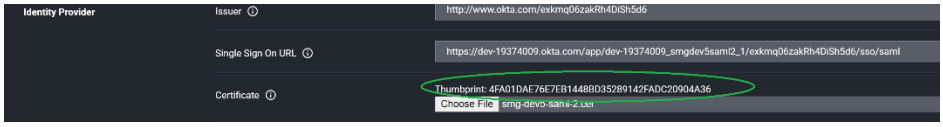
6. Click **Create**.



7. Under **Identity Provider | Single Sign On URL** enter the URL from the setup instructions.



8. Under **Certificate**, select the certificate you saved earlier.
9. From the **Binding** drop-down, select **HTTP Post**.
10. Under **Privilege Manager Entity ID** match what you entered in the app setup for Audience URI (SP Entity ID), for example *PrivilegeManagerServiceProvider*, if you went with the default suggestion.
11. Under **Privilege Manager URL**, enter your instance URL, for example `https://myprivilegemanger/Tms/`.
12. Click **Save Changes**.



Note: After saving the identity provider, Privilege Managershows the certificate thumbprint in the UI. It should match what Windows shows for the thumbprint on the certificate downloaded from Okta:

Configure User Options

Normally you need to create a new Federated user that matches an Okta username. But you can optionally have Privilege Managermatch AD users by `DOMAIN\username` and/or create new Federated users automatically.

Match Active Directory Users

If you select this option, you must configure Okta to send users in the format `DOMAIN\username` or `username@domaindnsname`. You should import users (and groups if desired) from AD, and add the desired user(s) to one or more Privilege ManagerRoles before attempting to sign in.

Create Users Automatically

When this option is selected, Privilege Managerwill create a new Federated user whenever a username cannot be matched to an existing Federated user (or AD User if the option above is selected).

> **Note:** You'll still need to add the user to a Privilege Managerrole before they'll have any meaningful access. Support for group/role assertions is planned for a future release.

Managing Users

Create New Okta Users

If you don't have any Okta users, you'll need to go to the Okta Directory section and add them.

Okta requires the usernames be in the format of an email address. These are the usernames your users are going to use when they log into Privilege Manager. You can configure Okta to send Privilege Managera different username (like `domain\username`, or a short name like `yoda`).

Add Okta Users to Application

Before you can login, users must be assigned to the application in Okta.

1. Go to **Applications | Applications**.
2. Select your application.
3. Select **Assignments**.
4. Click assign and select one or more users.

> **Note:** After assigning a user, you can change the username to be whatever you want. Click the edit (pencil), and enter the username for your user (this only changes the username for this specific application).

Setup Active Directory Users

You can use Active Directory users that you've already imported into Privilege Manager.

> **Note:** After you've imported from Active Directory, you still need to add the AD users (or AD groups) to Privilege Managerroles.

Match by DOMAIN\username

Ensure the username in Okta matches the Global Identity data for the user in Privilege Manager.

Match by username@dnsdomainname

Ensure the username in Okta matches the Global Identity UserId in Privilege Manager, and the domain name part of the username matches the DNS domain name of the domain in Privilege Manager. We don't import this directly from AD, so we have to get it from the Global Identity and AD foreign system data.

Using GSuite as a SAML Provider

When configuring GSuite as a SAML Provider the basic steps to set up the foreign system are the same as provided under the "Setting up a SAML Integration" topic. There are a couple of extra points to note that might not be intuitive enough when following the Google documentation for the SAML setup.

External References

- Google: `https://support.google.com/a/answer/6087519`

Clarification of Steps in GSuite

When you are following the recommended steps to create a custom SAML application in GSuite, you will be shown a number of fields that you will need to use when configuring Privilege Manager. GSuite provides a test via their **SAML apps** | **Test** dialog. On that page in combination with an option to **Download Metadata**, the data provided needs to be used to edit/complete the GSuite foreign systems setup in Privilege Manager. It might be best to keep the GSuite app configuration page and Privilege ManagerConsole open in two different browser Windows for easy retrieval of data.

1. Go to your G-Suite app that you have configured in your browser and view the details.
2. Your browser URL, which will be similar to this `https://admin.google.com/u/1/ac/apps/saml/241286142839`, contains your **AppID**, which is the number string at the end of the URL, 241286142839 from this example.

   Copy your **AppID** from your URL. It needs to be added on the foreign systems page.
3. From the download metadata page, copy your **Entity ID** and and download the Certificate. You will need to upload this certificate in Privilege Managerlater.
4. For the **ACS URL** field, enter https://your-server.privilegemanagercloud.com/Tms/saml2/acs.
5. For the **Entity ID** field, enter PrivilegeManagerServiceProvider.
6. Leave the **Start URL** blank.
7. Check the **Signed** response box.
8. For the **Name ID Format** field, select **Email**.
9. For the **Name ID** field, select **Basic Information | Primary email**.

Steps in the Privilege ManagerConsole

1. In Privilege Manager, navigate to **Admin | Foreign Systems** and create a new SAML provider.
2. Enter values, for

a. **Issuer**, enter the Entity ID that was provided from your GSuite custom app.

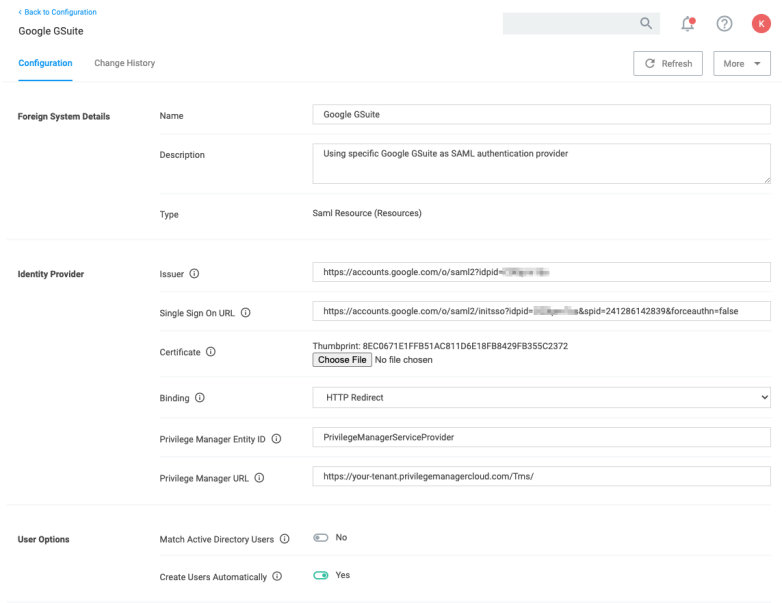
b. **Single Sign On URL**, enter the browser URL containing the **AppID** string as as `https://accounts.google.com/o/saml2/initsso?idpid=<idpid>&spid=<AppID>&forceauthn=false`.

   i. Replace `<AppID>` with your **AppID** value from step 2 under "Clarification of Steps in GSuite".

   ii. Replace `<idpid>` with your application's **Entity ID** from step 3.

c. **Certificate**, upload the downloaded certificate via **Choose File**.

3. Verify the page contains all the required data, refer to this example:



Next Step - Authentication Provider

To enable this new SAML provider to be used from the **Login** page, visit the **Authentication** tab and select your GSuite Foreign System from the listed providers. Refer to Managing Auth Providers.

> **Note:** After saving or enabling authentication providers, you may notice a short delay of unresponsiveness in your browser as the Privilege Managerapplication pools restart automatically.

Using Microsoft Entra ID as a SAML Provider

The SAML protocol requires the identity provider (Microsoft identity platform) and the service provider (the application) to exchange information. When configuring Microsoft Entra ID as a SAML provider, the basic steps to set up the foreign system are the same as provided in "Enter Application SAML Settings" on page 647.

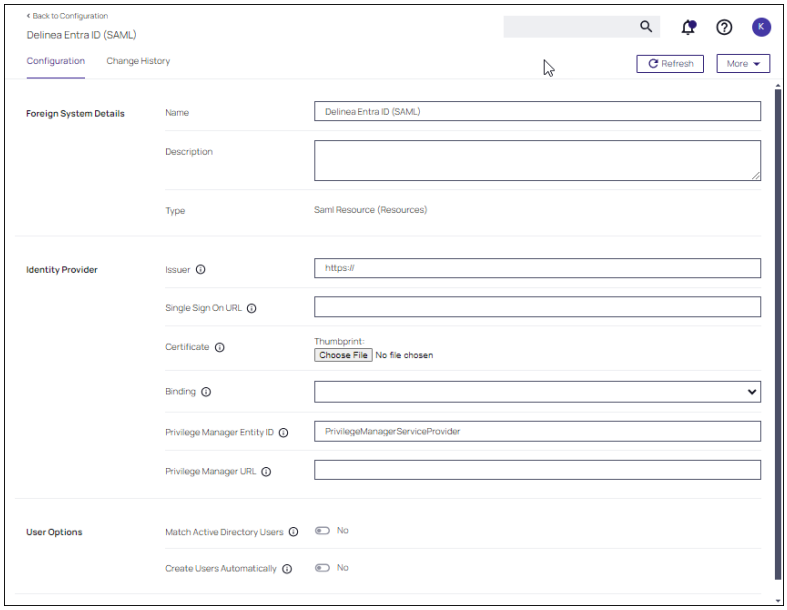
Prerequisites

- You will need access to your organization's Entra ID tenant. Refer to the Microsoft documentation if required.
- The Microsoft identity platform performs identity and access management (IAM) only for registered applications. Registering your new custom application establishes a trust relationship between your application and the Microsoft identity platform, with Entra.

  Refer to Register an application in Microsoft Entra ID for complete instructions for registering your custom application.
- Privilege Manager and Privilege Manager agent version 12.0 is required.

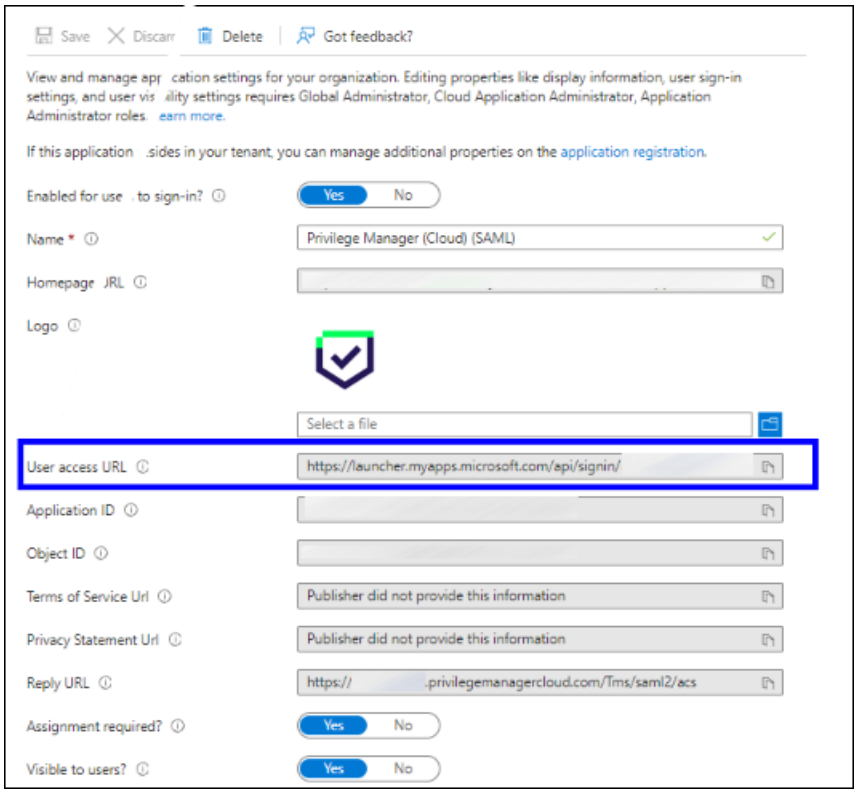
Configuring the SAML Provider

1. Select **Admin** | **Configuration** | **Foreign Systems**. Click **Create**.
2. Assign a **Name** for the provider and supply the **Identity Provider entity id**. Click **Create**.



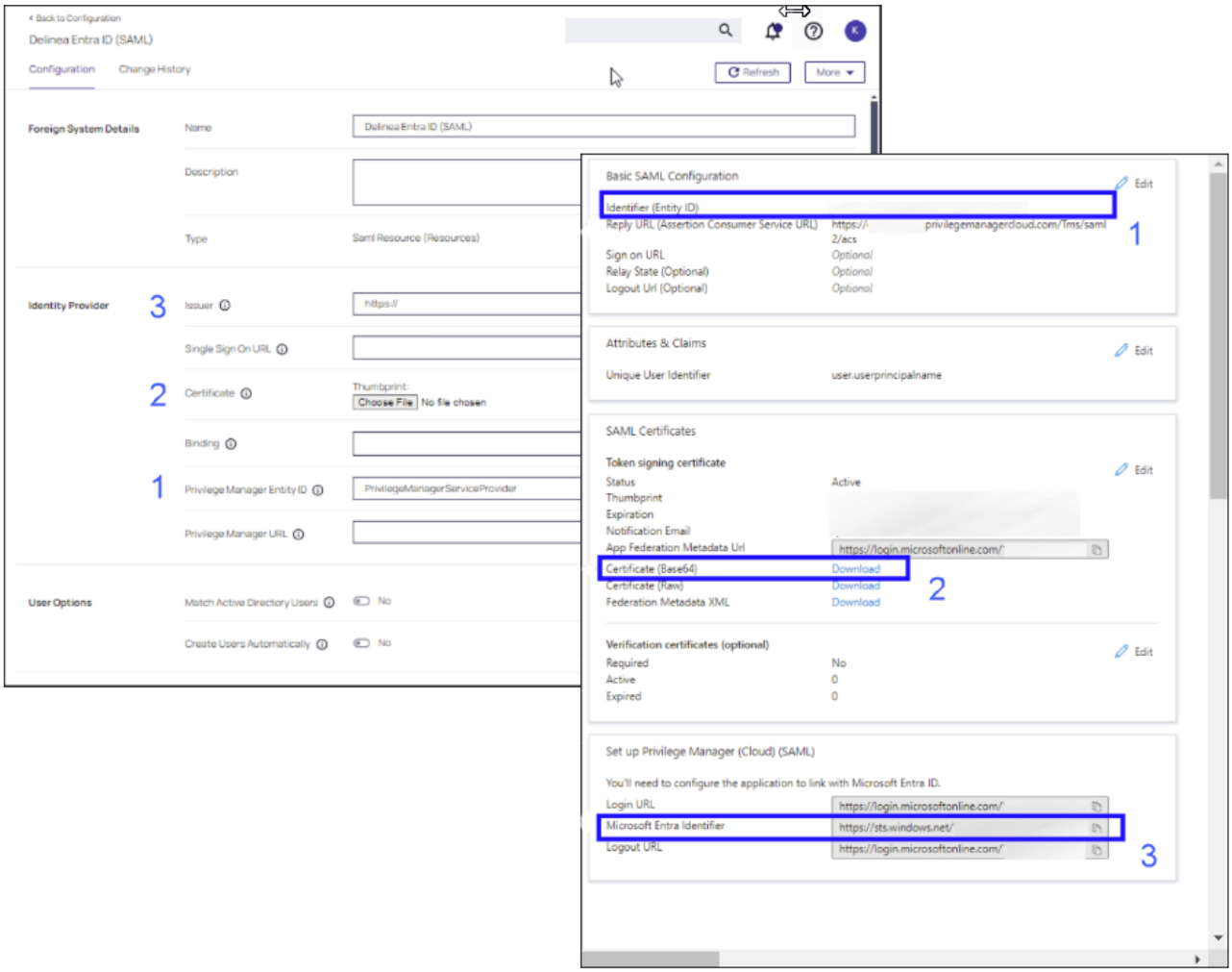
The **Identity Provider entity id** corresponds to the **User access URL** configured in your Entra ID tenant.

Privilege Manager Configuration	Entra ID Tenant
Identity Provider Entity id	**User access URL**



3. Enter the following parameters for your provider configuration.

Privilege Manager Configuration	Entra ID Tenant
Issuer	Microsoft Entra Identifier
Certificate	Certificate (Base 64)
Privilege Manager Entity ID	Identifier (Entity ID)



4. Set **Create Users Automatically** to **Yes**. For all users approved for this provider, a user account is automatically created. Click **Create**.

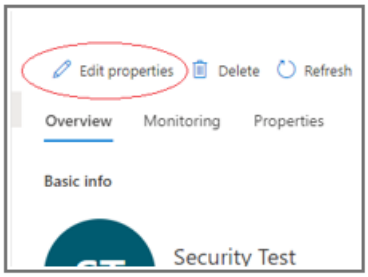
   Important: After the provider is created, you need to assign rights to these users.

Using Privilege Manager Mobile App with Hybrid SSO Logins

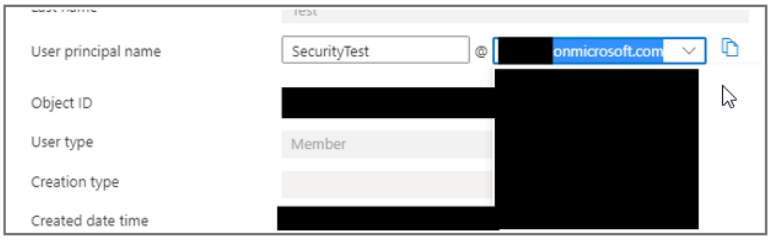
For situations where Azure AD is implemented in a hybrid cloud configuration with federation established to Okta for SSO logins, the use of the Privilege Manager mobile application will fail with the error message **Could not connect to management server**. In this situation, a user needs to be set up to bypass the Okta federation to login.

To bypass Okta federation with Office 365 in the above configuration, complete the following steps:

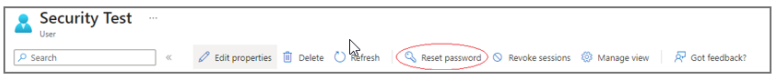
1. Create an on-premise user in Active Directory.
2. Sync the user to Azure AD, either manually or wait until an automatic sync occurs.
3. Locate the user in Azure AD and click **Edit Properties**.



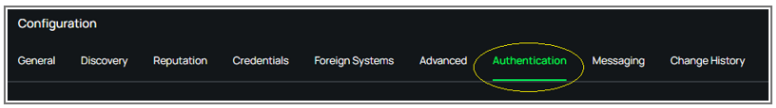
4. Under properties, locate the **User principal name** field and select an appropriate UPN domain at the drop-down. For example, .onmicrosoft.com.



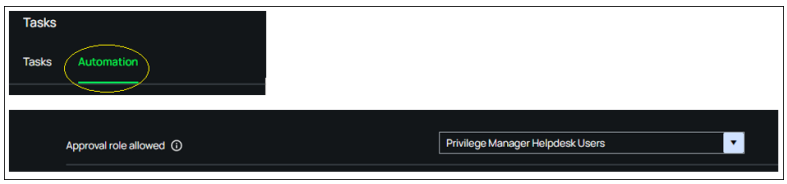
5. After changing the UPN, reset the password for the login account. An administrator can do this from the Azure console to get a temporary password to use.



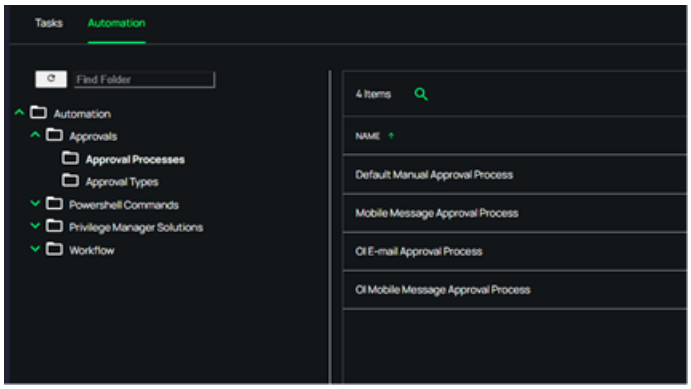
6. Ensure that Azure AD is enabled as an authentication source in Privilege Manager, in **Admin** | **Configuration** | **Foreign Systems**.



7. Ensure that any roles users will be added to have visibility into the approval queues visible in the application.

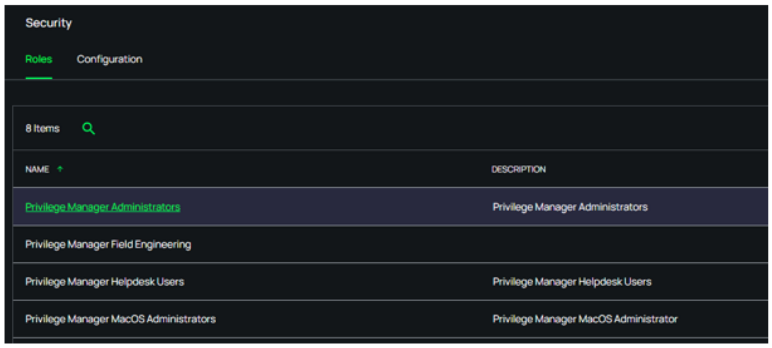


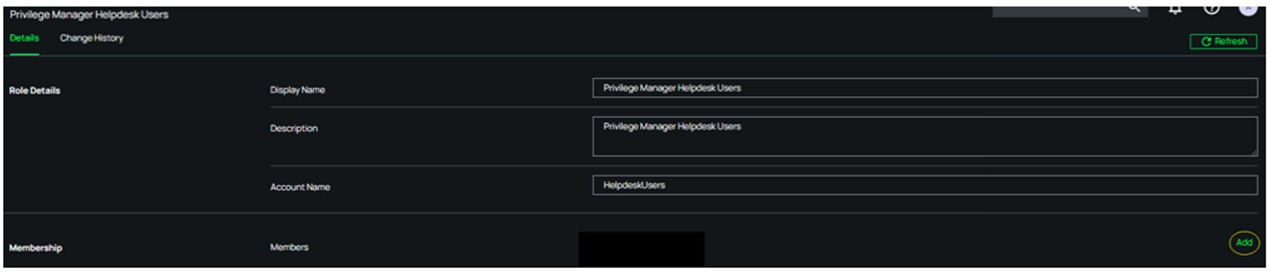
Automation Approval tasks are defined in **Admin** | **Tasks** | **Automation**.



8. Add the user to the desired role directly.

   Note: Do not add the user under **Admin** | **Users**, as it will not be recognized.



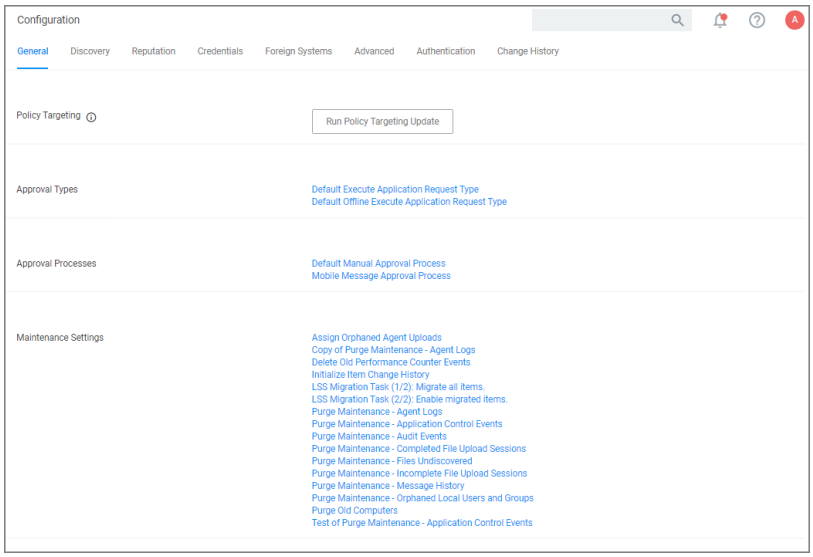


9. You can now log in to the Thycotic ACS application if all other configuration items have been completed.

   Note: It may be necessary to change **Local Authentication** on the service bus to enabled.

General Tab

The **General** tab provides a quick access to Privilege Manager Maintenance tasks and job settings.



Policy Targeting

The Policy Targeting Update automatically caches the list of policies applicable to each agent by updating the collections and resource targets.

Approval Types

For approval types can be specified as policy or file specific, a Security Rating System can be added, and a Process Handler can be entered. The following default approval types are available:

- Default Execute Application Request Type
- Default Offline Execute Application Request Type

Approval Processes

These are read-only items and by default Administrators are always allowed to approve any requests and an optionally activity can be started as part of the approval.

- Default Manual Approval Process
- Default Offline Approval Process
- Mobile Message Approval Process

Maintenance Settings

- Assign Orphaned Agent Uploads
- Delete Old Performance Counter Events
- Initialize Item Change History
- Purge Maintenance - Agent Logs
- Purge Maintenance - Application Events

- Purge Maintenance - Audit Events
- Purge Maintenance - Completed File Upload Sessions
- Purge Maintenance - Files Undiscovered
- Purge Maintenance - Incomplete File Upload Sessions
- Purge Maintenance - Message History
- Purge Old Computers

History Tab

The Change History tab is accessible via:

- **Admin | Configuration** – listing all changes made to Advanced, Authentication Provider, Foreign Systems, Discovery, and Reputation item configuration settings.
- **Admin | Policies** – listing all changes made to policies.
- Admin | More and then (for the default menu, might differ if customized)
  - **Filters** – listing all changes made to a specific filter.
  - **Actions** – listing all changes made to a specific action.
  - **Resources** – listing all changes made to a specific user editable resource. Meaning resources that are not user editable, like a file extension, do not have a history change tab.
  - **Tasks** – listing all changes made to a specific task.

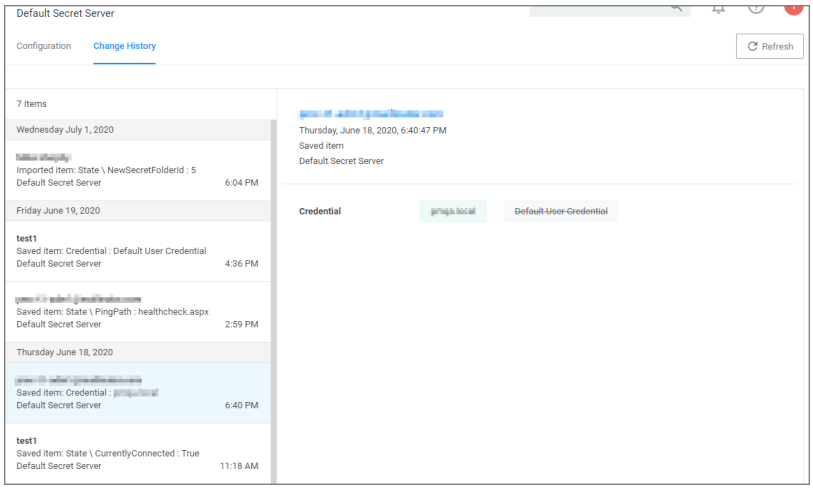
Once the tab is selected, it opens a two-column page. On the left all recorded changes are listed with the newest record on top. This left column data provides a summary of the changes:

- who made the change,
- what was changed,
- the type of change,
- item changed, and
- date/time of the change.

For any changes made to the Authentication Provider for Foreign Systems, like changing from NTLM to Azure Active Directory for example, the Change History provides details about the active and staged states with true and false indicators.

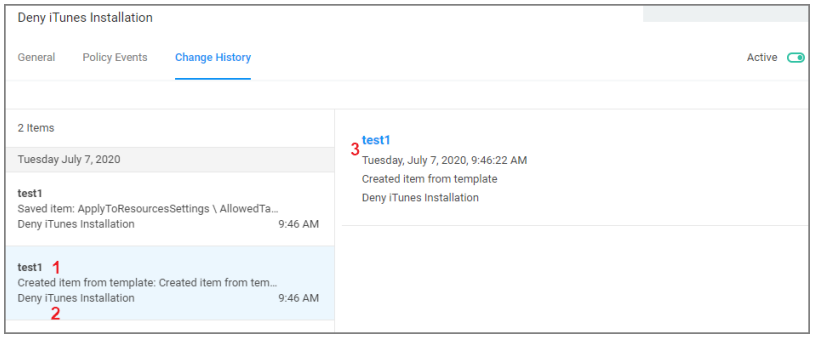
Looking at Details

The following image shows an example of the change history for a foreign system entry. The change shows that the foreign system was initially pointed at the local host URL, with a Credential and Client Secret pertaining to that localhost instance. An update was made to configure a real Secret Server instance URL with accompanying changes of Client Secret and Credential to be able to authenticate against that new URL.



Drilling Down

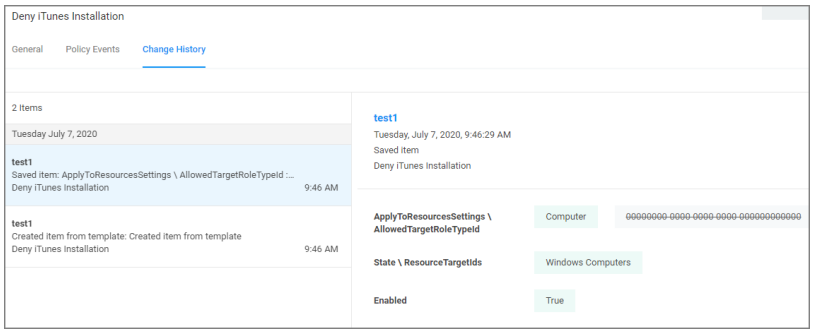
To look at details of any given change, select one of the change entries in the left column. For the example we created a policy to deny the installation of iTunes on Windows endpoints.



What we see:

1. Information about the system and user initiating the change, here *test1* and information about the type of change, here Created from template.
2. The name of the item that was created from template, the date and time when the change occurred.
3. Details on the summary information from the left, such as a link to view the user details and what change was done to which item.

The next screen shows a state change due to the policy being saved. The State\ResourceTargetIds are being saved for the first time for this policy.

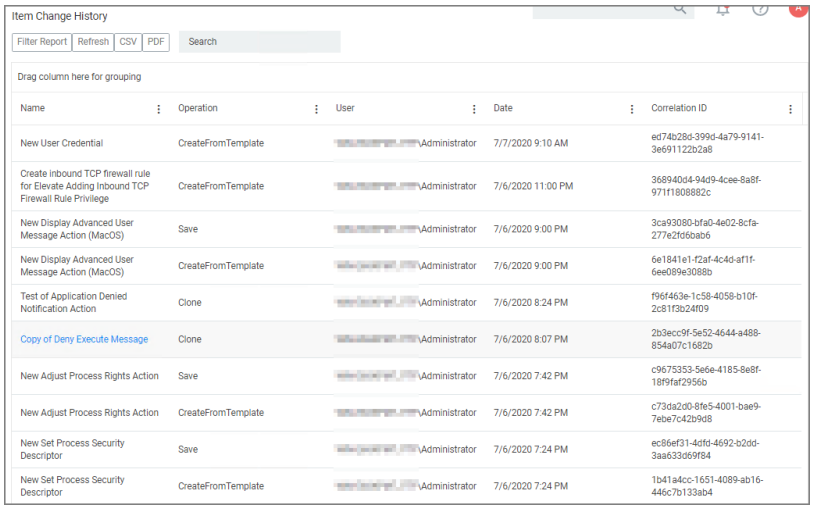


The last entry in the Change History list provides all the details about the change to the policy after initial creation and save.

Item Change History Report

The Item Change History Report is part of the **Diagnostic** group on the Reports page. You can also search for "change history" and the report will be listed on the search results page. Click the link to access the report.

The report lists the history of item changes.



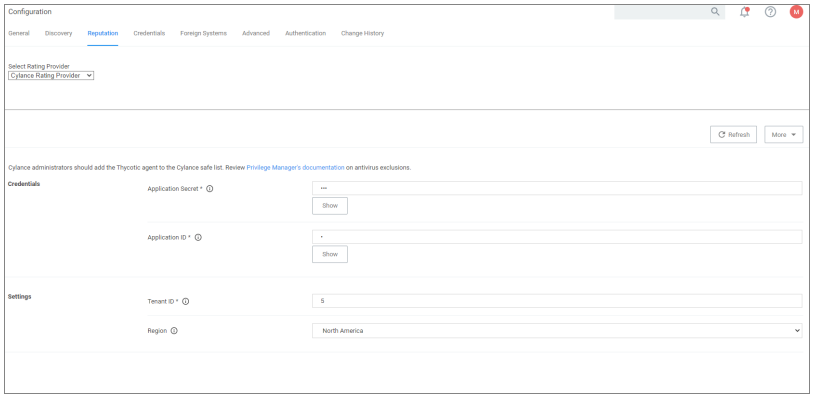
For further investigation, you can access the item that was changed by clicking the entries in the Name column.

Reputation Tab

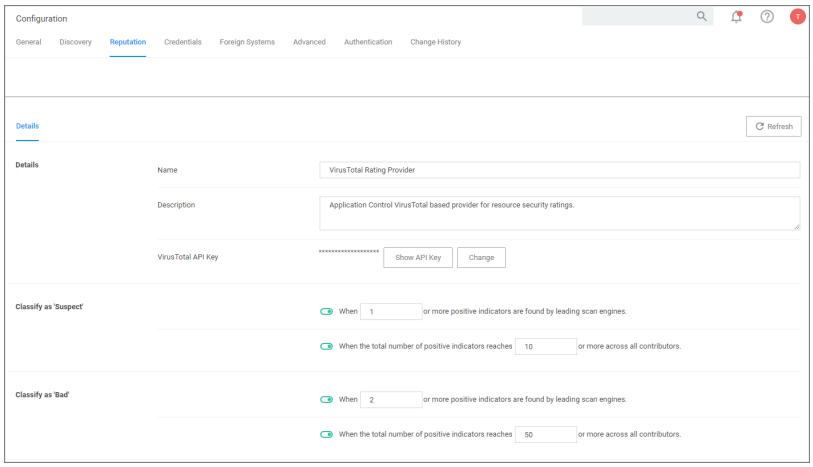
Here you select the Rating Provider from drop-down. Current options are Cylance and VirusTotal rating providers.

The configuration details required are different for the two rating providers as shown in the following sample images.

Cylance Rating Provider



VirusTotal Rating Provider



Configuration Feeds

Configuration Feeds are extensions to Privilege Manager. They allow Delinea to deliver new components/items to Privilege Manager on demand. Simply click through the options in the **Config Feeds** page.

1. Navigate to **Admin | Config Feeds**.
2. Browse the available config feeds by expanding **Privilege Manager Product Configuration Feeds**.

Expand the available product areas to drill-down into the configuration feeds available under:

- Application Control Solution
- Local Security Solution
- Delinea Management Server Core

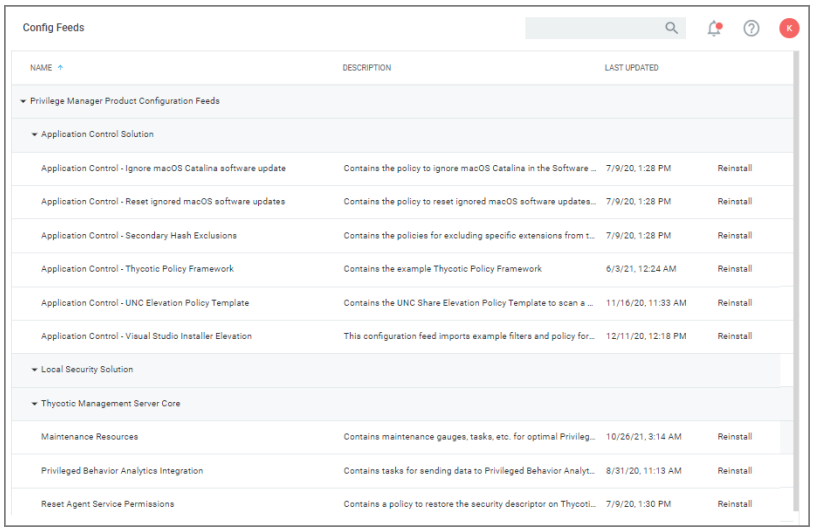
Solution	Feed	Description
Application Control Solution		Contains the policy to ignore macOS Catalina in the Software Update preference pane. Only works with the KEXT agent and Catalina, not supported with SYSEX agent or on Big Sur and up.
	Reset ignored macOS Software Updates	Contains the policy to reset ignored macOS software updates in the Software Update preference pane.
	Secondary File Hash Exclusion Policy	Policy template to exclude non-executable files from the hash process.
	Delinea Policy Framework	Contains the example Delinea Policy Framework. Installs 28 quick start policies.
	UNC Elevation Policy Template	Contains the UNC Share Elevation Policy Template to scan a network share and automatically elevate MSI and EXE files.
	Visual Studio Installer Elevation	Contains example filters and a policy for elevating Visual Studio Installers. After the installation the policy needs to be activated. Note: For enhanced security, the policy should include a certificate filter when rolled out into a production environment.
Delinea Management Server Core	Maintenance Resources	Contains maintenance gauges, tasks, etc. for optimal TMS performance.

Solution	Feed	Description
	PrivilegedBehaviorAnalytics Integration	Contains tasks for sending data to Privileged Behavior Analytics (PBA) - requires a SysLog Foreign System to be configured.
	Reset Agent Service Permissions	Contains a policy to restore the security descriptor on Delinea Services for Privilege Manager versions prior to v10.7.1.
	SQL CPU Usage Gauge	Contains a gauge and report to monitor SQL CPU usage.
	Windows Server and Desktop Filters	Contains Windows Server and Desktop Filters.
	Remove Active Directory Domain	Contains a task that deletes an Active Directory domain from the foreign systems tab, along with its child items.
	Merge Duplicate Active Directory Domains	Contains a task that merges duplicate Active Directory Domains, so that Organizational Units and their policies are correctly represented.
	Purge Old Unmanaged AD Computers	Contains a task that will delete unmanaged computers, imported from Active Directory, that have not been updated in 90 days by default.

Installation, Re-installation, and Updates

There are three potential options for each of the Configuration Feeds.

- Install: This is the available option for new configuration feeds or when the configuration feed has not previously been installed on the Privilege Manager instance.
- Reinstall: This option is shown when the configuration feed has previously been installed on the Privilege Manager instance.
- Update: This option is shown when the configuration feed has previously been installed on the Privilege Manager instance and an update to the configuration feed is available.

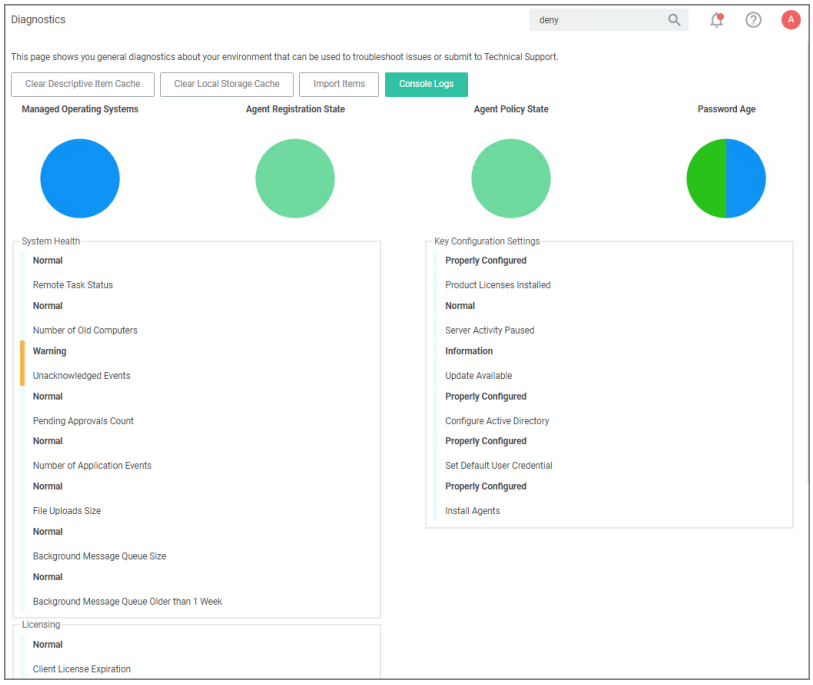


Note: If items from a configuration feed are used and have been customized, any re-installation or update will overwrite those customizations. Always rename modified items or save a copy to provide accidental overwriting.

Diagnostics Page

Navigate to the **Admin | Diagnostics** page to view more comprehensive system details. Select any of the gauges to drilldown into details.

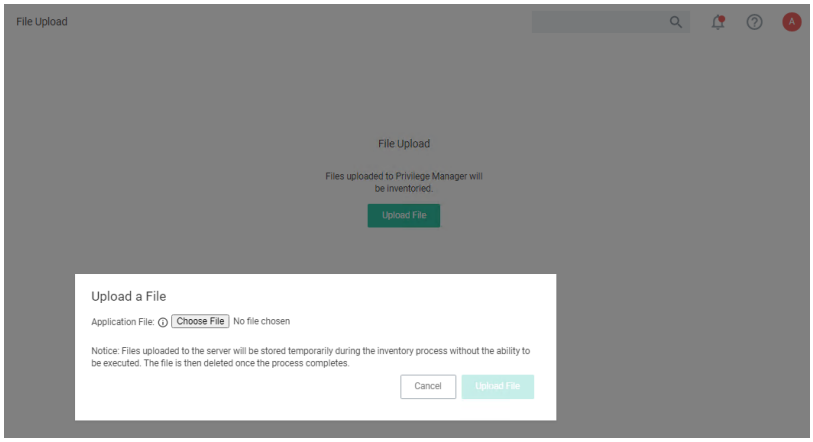
The Diagnostics page is also the go-to stop for full system health. Go there to find Server Console Logs and other system level warnings or tips.



The Licensing area provides information about expired licenses, exceeded license counts, and limits for each operating system.

File Upload

The File Upload options allows existing file uploads via the standard Choose File dialog.



The file upload functionality is available during imports of items, for diagnostics, and for inventory purposes.

Filters

In Privilege Manager, using a robust filtering system is the key to creating accurate and effective Policies.

A filter is made up of specific criteria that Privilege Manager uses to target important file data (or Events) that occur across your environment. You can think of Filters as the core identifiers in your Privilege Manager system. They are used to identify various levels of activity across your organization's computers, including processes (applications) that are launched on computers, who is executing an application, or the state of the computer that the process is being executed on.

An Event in Privilege Manager is any piece of file data or executable on a computer that is targeted by a policy.

There are different methods for Filter-creation and usage, but if you take the time to familiarize yourself with our out-of-the-box filters they can help make your policy-creation process easy. This article will provide details and descriptions for Windows Filters in Privilege Manager and how you can begin using out-of-the-box Filters, or create your own.

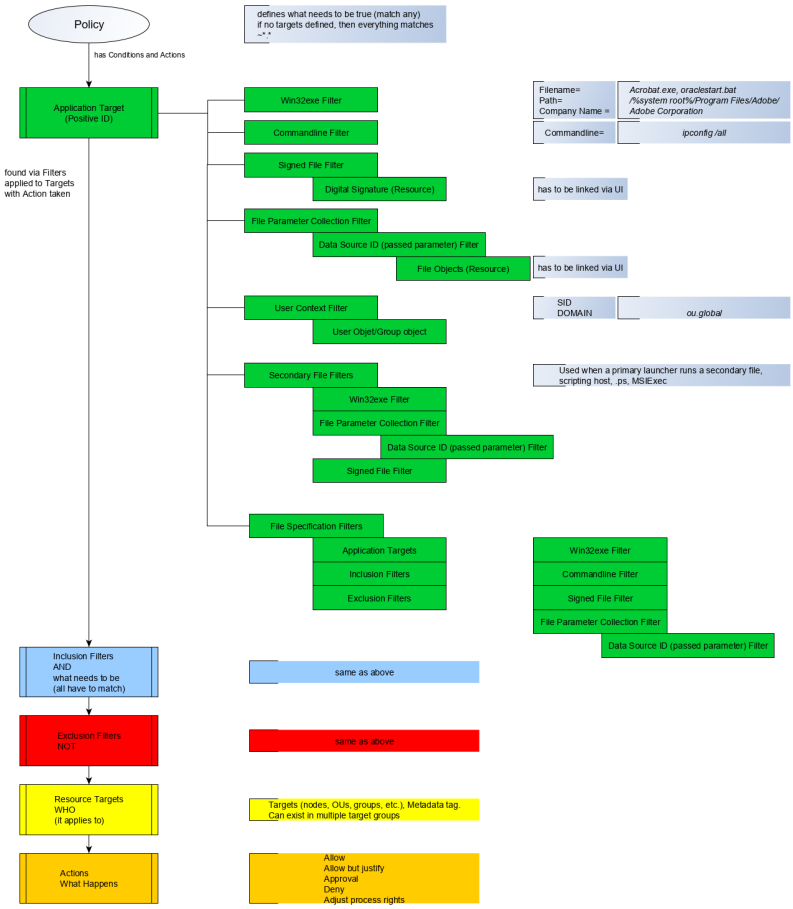
Types of Filters

We recommend leveraging Privilege Manager's out-of-the-box filters to get your policies up and running fast! For a complete list of out-of-the-box filters according to category type, review our Filters' Catalog for Privilege Manager here.

You can search your full list of available filters by navigating to **Admin | Filters** in Privilege Manager. If you already know what you want to target, simply try typing keywords in the search bar to check whether a filter exists that fits your target goal.

Note: If using the default filters provided with Privilege Manager, always verify existing targeting information.

Review the Filters Catalog for Privilege Manager for details about all out-of-the-box filters shipped with the product.



Create A Copy - How to Use Filter Templates

Out-of-the-Box filters are designed to be used as templates, meaning when you open these filters you will see a **Duplicate** option rather than the option to immediately Edit. These filter templates are protected to provide a jumping off point whenever creating new filters. They are formed by specific criteria that you can tailor according to your specific use case after copying.

Keep in mind that every filter in Privilege Manager - whether or not it is a template - can be leveraged by the Copying feature.

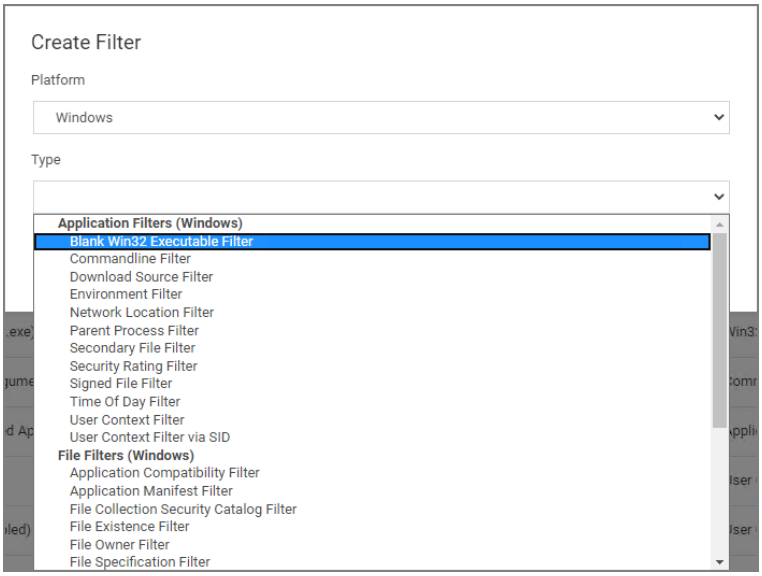
Creating a New Filter Manually

The following a basic steps to create a filter. Based on platform and type the end result shown in this example can be different.

1. In the Privilege Manager console, navigate to **Admin | Filters**.
2. Click **Create Filter**.
3. On the **Create Filter** modal,
   a. select a Platform from the drop-down.

   Options here are:
   - Windows
   - macOS
   - Unix/Linux

   b. select the Type from the drop-down.

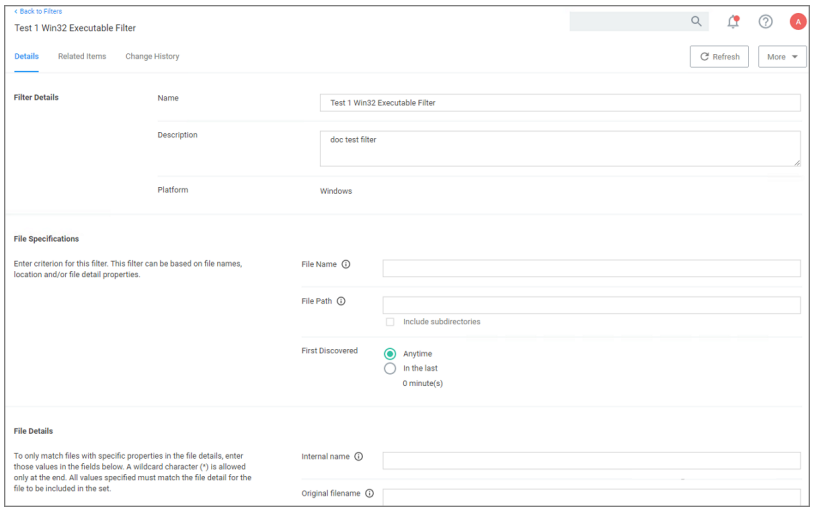


   The Type depends on the platform selection.

c. enter a **Name** and **Description**.

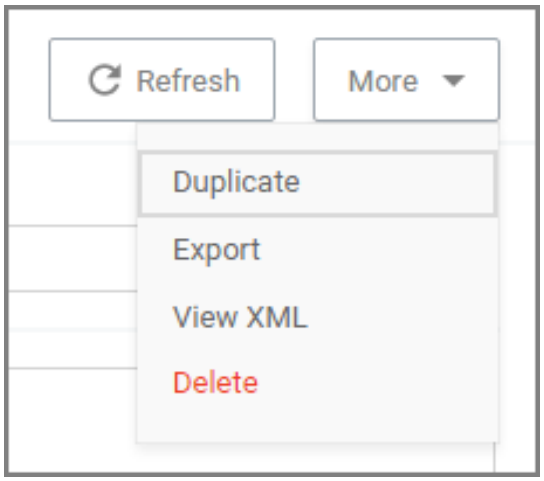
4. Click **Create**.

Once the filter is created, the new filter page open and information under the Details, File Specifications, and File Details sections can be edited. The Save and Cancel buttons appear once you make the first change on the page.



More Options Menu for Filters

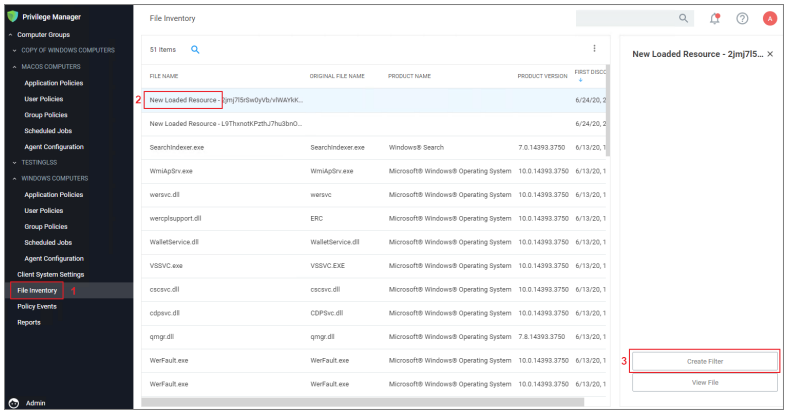
The **More** options menu offers users entry points to duplicate, export, view xml, and delete filters that are already on the system.



Creating New Filters using Event Discovery

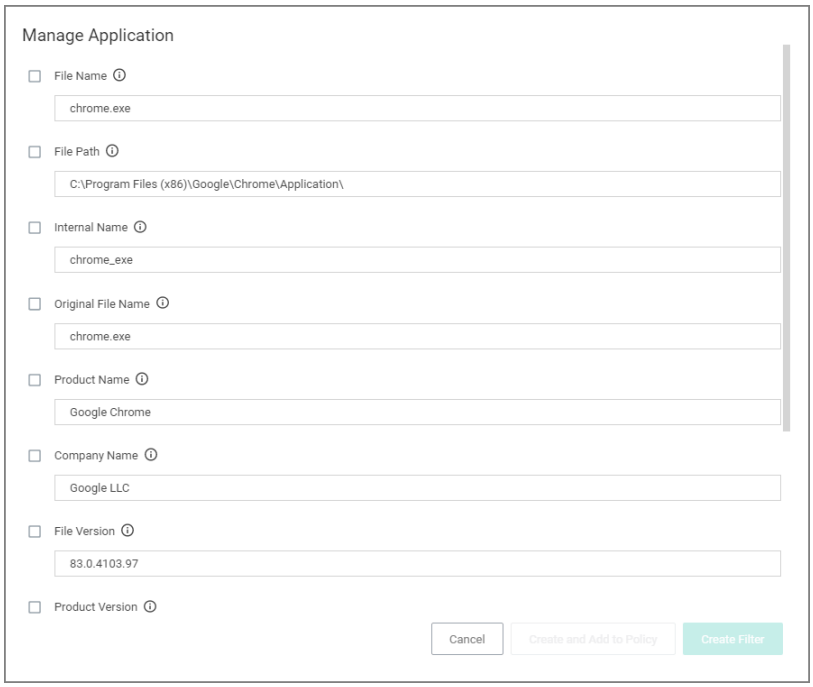
One way to begin creating new Filters that identify specific files or applications on your network is to set up a Learning Mode Policy and use the events pulled in by Privilege Manager from actions performed on a test machine. Refer to Event Discovery for more information on setting up a Learning Mode Policy.

1. In Privilege Manager, navigate to **File Inventory**.



2. Select a recognized event.
3. Click **Create Filter**.

This brings you to the **Manage Application** modal with the known identifiers needed for targeting this specific event auto-populated, for this example chrome.exe.



The modal has options to **Create and Add to Policy** or to just **Create Filter**.

> **Note:** If you are NOT directed to such a dialog, this means Privilege Manager doesn't have enough information to target this event yet. In these cases you may need to create Filters manually.

The dialog reveals the available list of building blocks, attributes, or criteria used for creating a filter. In other words, the following list of criteria are possible data fields that Privilege Manager can look and sift through for on any given event that your policies target for Windows machines. Note that criteria can vary depending on the type of filter you are creating:

- File Name
- Path
- Internal Name
- Original File Name
- File Version
- Product Name
- Product Version
- Company Name
- File Signature (File must be signed by)

You can choose which criteria to use by checking or un-checking any of the available check boxes on the dialog. If you are new to the filter creation process, we recommend experimenting with these different identifiers in your test environment to ensure that you are using a comprehensive list of identifiers in your filter, enough to target the application or file intended but not too specific that variations to your target will fall through the filter's criteria hooks.

List of Default Filters

This topic provides the Privilege Manager filters catalog for all out-of-the-box filters that are baked into Privilege Manager and can be used to make your policy configuration process easy.

Win32 Executable Filters

Filter	Description
Add Hardware Utility (hdwwwiz.exe)	Filter used to identify the Device Pairing Wizard that appears when you click Add Device in Windows Vista and Windows 7
AOL Instant Messenger	Filter used to detect AOL Messenger
AppCmd for App Pool Recycling (appcmd.exe)	Filter used to identify the AppCmd executable
Backup and Restore Utility (sdcit.exe)	Filter used to identify the Windows Backup and Restore utility
Chrome	Filter used to detect Google Chrome web browsers
COM Elevation Host Utility (COMElevateHost.exe)	Filter to detect the COMElevateHost. This is used to detect when COM components are being elevated, such as the Network Adapter Properties
Command Processor (cmd.exe)	Filter used to identify the Windows command shell processor
Control Panel Utility (control.exe)	Filter used to identify the process used to launch Control Panel applets
Defragment GUI Utility (dfrgui.exe)	Filter used to identify the disk defragment utility within Windows
Device Pairing Wizard	Filter used to identity the Device Pairing Wizard that appears when you click Add Device in Windows Vista and Windows 7
Eudora	Filter used to detect Eudora email client
Firefox	Filter used to detect Firefox web browsers
Google Talk	Filter used to detect Google Talk
IIS Manager Executable Filter (inetmgr.exe)	Filter used to identify the IIS Manager executable
IIS Reset Executable Filter (iisreset.exe)	Filter used to identify the IIS Reset executable

Filter	Description
Internet Explorer	Filter used to detect Internet Explorer web browsers
ISCSI Executable Filter (iscsicpl.exe)	Filter used to identify the ISCSI executable
iTunes	Filter used to detect iTunes
Library Loader Utility (rundll32.exe)	Filter used to identify the dynamic library loader utility used by Windows to launch various system configuration applets
Microsoft Installer File Filter	Filter used to detect the Microsoft Installer. This filter can be used in policies with secondary file filters targeting specific MSI files
Microsoft Management Console (mmc.exe)	Filter used to identify the Microsoft Management Console Utility
Microsoft Windows Media Player	Filter used to detect Windows Media Player
MS Access	Filter used to detect Microsoft Access
MS Excel	Filter used to detect Microsoft Excel
MS FrontPage	Filter used to detect Microsoft FrontPage
MS InfoPath	Filter used to detect Microsoft InfoPath
MS Lync	Filter used to detect Microsoft Lync
MS OIS	Filter used to identify the Office Picture Manager Image Viewer
MS Outlook	Filter used to detect Microsoft Outlook
MS Powerpoint	Filter used to detect Microsoft PowerPoint
MS PPTVIEW	Filter used to detect Microsoft PowerPoint Viewer
MS Publisher	Filter used to detect Microsoft Publisher
MS Visio	Filter used to detect Microsoft Visio
MS VPreview	Filter used to detect Microsoft VPreview
MS Word	Filter used to detect Microsoft Word

Filter	Description
MSN Messenger	Filter used to detect MSN Messenger
NLB executable Filter (nlbmgr.exe)	Filter used to identify the NLB Manager executable
OODBC Executable Filter (odbcad32.exe)	Filter used to identify the OODBC executable
Opera	Filter used to detect the Opera Browser
Outlook Express	Filter used to detect Microsoft Outlook Express
Performance Monitor Utility (perfmon.exe)	Filter used to identify the Performance Monitor launcher stub utility within Windows
Powershell (powershell.exe)	Filter used to identify the Windows Powershell command processor
Printer Control Utility (printui.exe)	Filter used to identify the printer management applet launcher within Windows
QuickTime	Filter used to detect QuickTime
RealPlayer	Filter used to detect RealPlayer
Resource Monitor (resmon.exe)	Filter used to identify the Windows Resource Monitor application
Safari	Filter used to detect Apple Safari on Windows
Scripting Host (cscript.exe)	Filter used to identify the Windows Scripting Host command-line utility
Scripting Host (wscript.exe)	Filter used to identify the Windows Scripting Host commandline utility
Setup Display Languages Utility (lpksetup.exe)	Filter used to identify the Install/Uninstall of Display Languages setup utility for Windows
ShareX	This filter targets the ShareX application
Skype	Filter used to detect Skype
Trillian	Filter used to detect the Trillian application
User's Temp Directory Win32 Executable Filter	Filter used to target any executable (exe) in a user's temp directory

Filter	Description
Win32 Executables Discovered in the Last Week	This filter is limited to applications discovered on the endpoint within the last week
Winamp	Filter used to detect Winamp application
Windows Firewall (netsh.exe)	Filter used to identify the Windows Firewall netsh.exe
Windows Messenger	Filter used to detect Windows Messenger
Yahoo! Messenger	Filter used to detect Yahoo Messenger

Commandline Filters

Filter	Description
Add Printer Commandline Arguments	Filter used to identify the Add Printer UI applet
Azman.msc Commandline Filter for MMC Snap-in	Filter used to detect Windows Authorization Manager
Backup and Restore Commandline Arguments	Filter used to identify the Backup and Restore component, used as a commandline argument to a process
Certmgr.msc Commandline Filter for MMC Snap-in	Filter used to detect Windows Certificate Manager
Ciadv.msc Commandline Filter for MMC Snap-in	Filter used to detect Indexing Service Management
Compmgmt.msc Commandline Filter for MMC Snap-in	Filter used to detect Windows Computer Management
Defragment Component (dfrg.msc)	Filter used to detect the MMC Snap-in used to defragment disks in Windows XP
Devmgmt.msc Commandline Filter for MMC Snap-in	Filter used to detect Device Manager
Dhcpmgmt.msc Commandline Filter for MMC Snap-in	Filter used to detect DHCP Management

Filter	Description
Diskmgmt.msc Commandline Filter for MMC Snap-in	Filter used to detect Disk Management
Dnsmgmt.msc Commandline Filter for MMC Snap-in	Filter used to detect DNS Management
Eventvwr.msc Commandline Filter for MMC Snap-in	Filter used to detect Event Viewer
Fsmgmt.msc Commandline Filter for MMC Snap-in	Filter used to detect Shared Folders Management
Fsrm.msc Commandline Filter for MMC Snap-in	Filter used to detect File Resource Manager
Gpedit.msc Commandline Filter for MMC Snap-in	Filter used to detect Group Policy Editor
Hardware Wizard Applet	Filter used to identify a commandline argument referring to the Control Panel applet used to add new hardware
Lusrmgr.msc Commandline Filter for MMC Snap-in	Filter used to detect Local User and Group Management
Napclfcfg.msc Commandline Filter for MMC Snap-in	Filter used to detect NAP Client Configuration
Network Adapter Elevate Attempt	Filter used to detect when a user right-clicks on a network adapter and selects Properties
Ntmsmgr.msc Commandline Filter for MMC Snap-in	Filter used to detect Removable Storage Manager
Performance Monitor Component (perfmon.msc)	Filter used to detect Performance Monitor
Printmanagement.msc Commandline Filter for MMC Snap-in	Filter used to detect Print Management
Recycle App Pool Commandline	Filter used to identify the recycle command for application pools
Rsop.msc Commandline Filter for MMC Snap-in	Filter used to detect Resultant Set of Policy

Filter	Description
Secpol.msc Commandline Filter for MMC Snap-in	Filter used to detect Local Security Settings Manager
Services.msc Commandline Filter for MMC Snap-in	Filter used to detect Services Manager
Sqlservermanager12.msc Commandline Filter for MMC Snap-in	Filter used to detect SQL Server Manager
System Control Panel Applet	Filter used to identify a commandline argument referring to the Control Panel applet used to change the system time and date settings
Tpm.msc Commandline Filter for MMC Snap-in	Filter used to detect Trusted Platform Module Management
Wbadmin.msc Commandline Filter for MMC Snap-in	Filter used to detect Windows Server Backup
Wf.msc Commandline Filter for MMC Snap-in	Filter used to detect Windows Firewall Management
Wmimgmt.msc Commandline Filter for MMC Snap-in	Filter used to detect WMI Management

Environment Filters

Filter	Description
Manual Application Compatibility Setting	Detects whether an application is being run with manual override options
User Access Control Consent Dialog Detected	This filter will match when an application that requires User Access Control consent is launched
User Requested Run As Administrator	Detects whether a user has right-clicked on an application and used Delinea's custom ‘Request Run as Administrator' option

Network Location Filters

Filter	Description
Disconnected from Network	Filter used to detect when the computer is not attached to a network

Filter	Description
Domain Network Location Filter	Filter used to detect when the computer is attached to a network classified as domain
Private Network Location Filter	Filter used to detect when the computer is attached to a network classified as private
Public Network Location Filter	Filter used to detect when the computer is attached to a network classified as public

Parent Process Filters

Filter	Description
Thycotic Copy/Installer Helper Parent Process Filter	Filter used to detect when a user attempts to copy a file using the Privilege Manager copy helper

Secondary File Filters

Filter	Description
Target MSI and Scripts executed from the User's Temp Directory	Filter used to target MSI and Scripts executed from the User's Temp Directory

Security Rating Filters

Filter	Description
VirusTotal	This filter will target VirusTotal for Reputation Checking
VirusTotal-Bad Rating	This filter will target VirusTotal for Reputation Checking
VirusTotal-Clean Rating	This filter will target VirusTotal for Reputation Checking
VirusTotal-Suspect Rating	This filter will target VirusTotal for Reputation Checking

VirusTotal Filters based on configuring VirusTotal integration in Privilege Manager. For steps to do this, see our *VirusTotal Integration Guide here*

Time of Day Filters

Filter	Description
Business Hours (8:30AM to 5:30PM)	This filter is limited to 8AM to 6PM weekdays

Filter	Description
Business Hours (8AM to 6PM)	This filter is limited to 8AM to 6PM weekdays
Business Hours (9AM to 5PM)	This filter is limited to 9AM to 5PM weekdays
Weekends	This filter is limited to weekends

User Context Filters

Filter	Description
Administrators	Detects when an application is running with elevated (administrator) permissions
Administrators (Include Disabled)	Detects when an application has an administrator user token

File Filters

Application Compatibility File Filters

Filter	Description
Administrative Rights Required Application Compatibility Filter	This filter tests whether Windows has detected that this executable requires administrative rights
Generic Installer Detection Filter	This filter indicates that Windows has detected that an executable is an Application Setup
Highest Available Application Compatibility Filter	This filter tests whether Windows has detected that this executable required highest available rights
Specific Installer Detection Filter	This filter indicates that Windows has detected that an executable is an Application Setup
Specific Non Installer Detection Filter	This filter indicates that an executable has been flagged as not being an Application Setup

Manifest Filters

Filter	Description
Require Administrator Rights Manifest Filter	This filter tests whether an executable is marked as requiring Administrative rights

Filter	Description
Require Highest Available Rights Manifest Filter	This filter tests whether an executable is marked as requiring highest available rights
Manifest Present Filter	This filter tests whether an executable has a security manifest

File Owner Filters

Filter	Description
System (Wheel) File Owner	Files that are owned by the Wheel Group (Unix)
System File Owner Filter	Filter used to detect files owned by the System account
Trusted Installer File Owner Filter	Filter used to detect files owned by the Trusted File Owner account

File Specification Filters

Filter	Description
Any Package (macOS)	Target .pkg and .mpkg files
App Store Preference Pane (macOS)	Filter used to detect App Store Preference Pane in macOS
Common Executable Folders	Filter used to detect files in common executable directories, such as C:\Windows, C:\Program Files, and C:\Program Files(x86)
Date and Time Preference Pane (macOS)	Date and Time Preference Pane (macOS)
Default App Bundles File Specification Filter	The default filter for discovering app bundles on macOS
Default File Specification (All executable types)	Specifies all executable file types in Windows and Program files
Default File Specification (macOS)	The default filter for discovering executable files on macOS
Default File Specification (Windows)	This specifies executables in Windows and Program files
Documents and Settings	Filter used to detect files in the Downloaded Program Files directory

Filter	Description
Drivers	Filter used to detect files in the C:\Windows\System32\drivers directory
Energy Saver Preference Pane (macOS)	Filter used to detect the Energy Saver Preference Pane in macOS
Executables in Windows Directories	This specifies executables in Windows directories
Executables in Windows Directories (All executable types)	Specifies all executable file types in Windows directories that are not present in a signed security catalog
macOS/Users/File Specification	The default filter for files in the /Users/directory on macOS
Network Drive Filter	Specifies files present on network file systems
Optical Drive Filter (CD/DVD)	Specifies files present on optical drives (CD/DVD)
Parental Controls Preference Pane (macOS)	Filter used to detect the Parental Controls Preference Pane in macOS
Printers and Scanners Preference Pane (macOS)	Filter used to detect the Printers and Scanners Preference Pane in macOS
Program Data	Filter used to detect files in the C:\ProgramData\ directory
Program Files	Filter used to detect files in the C:\Program Files\ directory
Program Files (x64 on Win32)	Filter used to detect files in the C:\Program Files\ directory
Program Files (x86)	Filter used to detect files in the C:\Program Files(x86)\ directory
Removable Drive Filter	Filters files present on removable drives such as Floppy Drives and USB devices
Security and Privacy Preference Pane (macOS)	Filter used to detect Security and Privacy Preference Pane in macOS
Sharing Preference Pane (macOS)	Filter used to detect the Sharing Preference Pane in macOS
System Catalog Folder	Filter used to detect files in the CatRoot directory
System Preferences (macOS)	Filter used to detect the System Preferences Preference Pane in macOS
Temporary ASP.NET 1.0 Files	Filter used to detect files in the .NET 1 Temp directory

Filter	Description
Temporary ASP.NET 1.1 Files	Filter used to detect files in the .NET 1.1 Temp directory
Temporary ASP.NET 2.0 Files	Filter used to detect files in the .NET 2 Temp directory
Temporary Files	Filter used to detect files in the C:\Windows\Temp directory
Thycotic Copy/Installer Helper Application	Filter used to detect usage of the Privilege Manager copy helper
Time Machine Preference Pane (macOS)	Filter used to detect the Time Machine Preference Pane in macOS
Uncommon Executables Folders	Filter used to detect files in the Uncommon directories
Users and Groups Preference Pane (macOS)	Filter used to detect the Users and Groups Preference Pane in macOS
User's Directory Collection File Specification Filter	Used to target any file in the user's temp directory
User's Downloads Directory File Specification Filter	Used to target any file in the user's temp directory
User's Temp Directory File Specification Filter	Used to target any file in the user's temp directory
Windows Directory	Filter used to detect files in the C:\Windows directory
Windows Directory (Include Subdirectories)	Filter used to detect files in the C:\Windows\ directory
Windows Dll Cache	Filter used to detect files in the C:\Windows\System32\dllcache directory
Windows Side By Side	Filter used to detect files in the C:\Windows\WinSxS\ directory
Windows Software Distribution	Filter used to detect files in the Windows Software Distribution directory
Windows\System32	Filter used to detect files in the C:\Windows\System32 directory
Windows\System32 (Include Subdirectories)	Filter used to detect files in the C:\Windows\System32\ directory
Windows\SysWOW64	Filter used to detect files in the SysWOW64 directory
Windows\SysWOW64 (Include Subdirectories)	Filter used to detect files in the SysWOW64\ directory

Security Catalog Filters

Filter	Description
Present in Signed Security Catalog	Filter used to detect Operating System Files and other trusted files dynamically on each system by using that machine's Signed Security Catalog. This filter does not need to be modified on the server

Miscellaneous Filters

App Bundle Filters

Filter	Description
All Application Bundles Filter (macOS)	Filter used to detect All Applications Bundles

Coff Header Filters

Filter	Description
32-bit Executables	Filter used to detect files with the 32-bit executable machine type header set
All Executable Types	This filter includes all executable types
Commandline Executables	Filter used to detect files with the Windows console subsystem header set
GUI Executables	Filter used to detect files with the GUI header set
Native Executables	Filter used to detect files with the executable header set
Windows CE Executables	Filter used to detect files with the Windows CE Subtype header set
Program File Executables	Filter used to detect files with the executable or DLL header set
Posix Executables	Filter used to detect files with the POSIX header set
X64 Executables	Filter used to detect files with x64 machine type header set

File Parameter Collections

Filter	Description
All Deny List Security Rated Applications	This collection contains all applications that have been denylisted by applying a security rating

Filter	Description
All Executables Discovered in Last 2 Weeks	Filter used to detect files that have been discovered by the server in the past 2 weeks
All Executables Discovered in Last Day	Filter used to detect files that have been discovered by the server in the past day
All Executables Discovered in Last Week	Filter used to detect files that have been discovered by the server in the past week
All Executables Discovered in Last Month	Filter used to detect files that have been discovered by the server in the past month
All Greylist Security Rated Applications	This collection contains all applications that are being monitored.
All Unclassified Applications	This collection contains all applications that have not been classified by a security rating. This filter has been removed from version 11.5.0, but remains available to customers who have this filter implemeted on an existing policy prior to version 11.5.0.
All Allow Listed Security Rated Applications	This collection contains all applications that have been allowed by applying a security rating

Mach-O Header Filters

Filter	Description
macOS DyLib	Identifies dynamic library (dylip) files according to their embedded Mach-O header (not specifically according to file name)
macOS Executables	Identifies files marked as executables according to their Mach-O header (not file mode changes via chmod)

Using RegEx in Filters

When using RegEx in Filters instead of a single file name or file specification, make sure to verify the syntax and test your filter before using it in production.

Examples of program names with versions in file names:

```
(flashutil[ a*zA*Z0*9\\.]+exe)
```

Winamp58_3660_beta_full_en*us

```
(winamp[ a*zA*Z0*9\\.]+exe)
```

Wireshark*win64*2.6.6.exe

```
(wireshark*win64*[ a*zA*Z0*9\\.]+exe)
```

Resource Targets and Collections

A Resource Target in Privilege Manager is a specified set of computers that meet certain criteria (e.g., type of operating system or location of the computers), meant to be used as targets for policies or scheduled tasks. To make a policy apply to a certain set of computers, you need a resource target comprising that set of computers and assign that resource target to the policy (or, to state it differently, assign the policy to the resource target).

There are several built-in resource targets (for example, "All 64-bit Windows Computers with Application Control Agent Installed") that can be used when defining policies so that users generally do not need to create custom resource targets. However, there are cases when the latter is needed and, toward that end, this article focuses on user defined resource targets.

Note: If you need to modify any items within Privilege Manager, duplicate the item and modify the duplicate instead of the built-in item so that an upgrade does not overwrite it.

This topic also briefly touches upon collections, a concept related to resource targets.

Resource targets are not the only kind of targets that can be assigned to policies; one could also assign an application filter to a policy to make the policy apply to the application file included in the filter.

User Defined Resource Targets

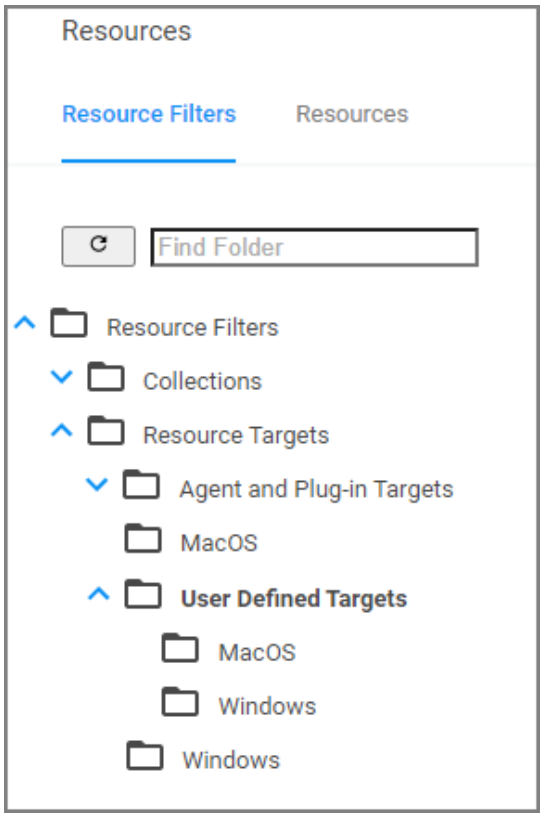
Targets are defined by starting with all known computers and then adding filters to narrow down the set (and after an initial narrowing down, if needed, expand it in some way).

You could create unique targets for all your policies, but if you want to create a target to be reused across multiple policies, it will be more practical to follow these steps.

Interface to View or Create/Modify User Defined Targets

In the Privilege Manager console, navigate to **Admin | Resources** . On the Resources page select the **Resource Filters** tab, then in the tree go to **Resource Filters | Resource Targets | User Defined Targets**, and select either macOS or Windows.

If you already created user defined targets, you see them listed here and can modify any of them by clicking the name and then editing the definition.



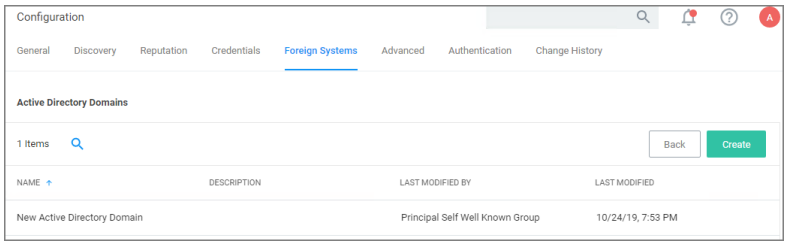
Performance Considerations

Resource Targets are reevaluated when the scheduled task **Collection and Resource Targeting Update** runs. This operation is expensive for large numbers of computers. To keep performance high we suggest that you keep the overall number of targets to a minimum. Also note that targets with simpler definitions are generally less expensive.

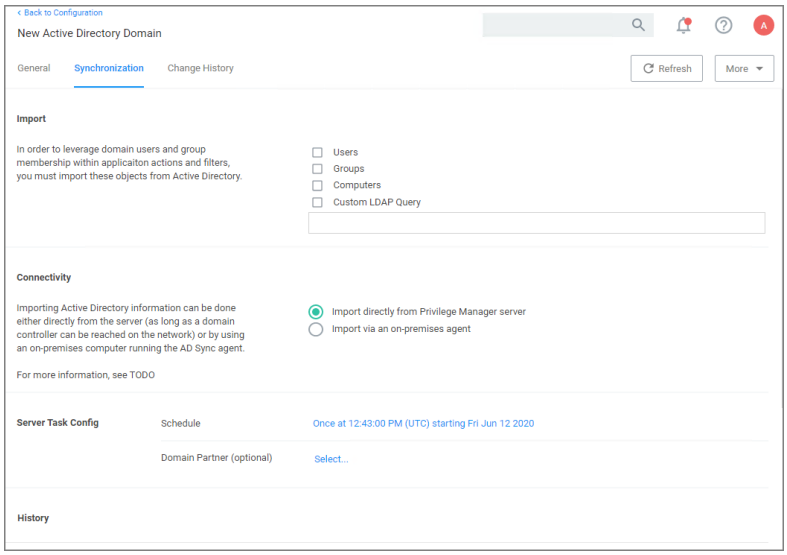
Active Directory as Related to Resource Targets

After you have created an Active Directory (AD) instance in Privilege Manager, you need to import computers (computer records, to be more precise).

1. Navigate to **Admin | Configuration | Foreign Systems**.



2. Select your AD instance and navigate to the **Synchronization** tab.

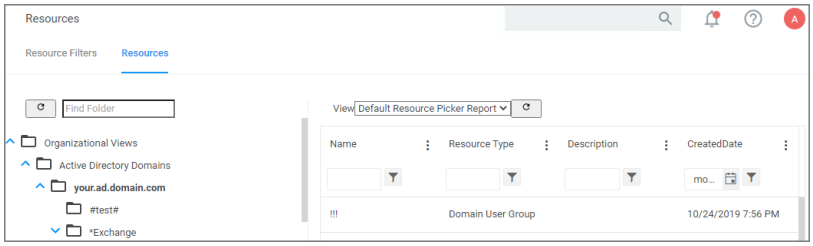


a. Under **Import** select which objects you want to import from your AD instance.
   - If you select Computers, the default import task also imports the Organization Units (OU) to which the computers belong.
   - If you select LDAP query, enter the query in the text field.

b. Under **Connectivity** select your import path. Import either directly from the server (as long as a domain controller can be reached on the network) or by using an on-premises computer running the "Directory Services Agent (AD)" on page 73.

3. Click **Save**.

After the task completes, navigate to **Admin | Resources**, select the **Resource** tab. In the tree under **Organizational Views | Active Directory Domains | (your AD name)**, you should be able to see your OUs and computers.

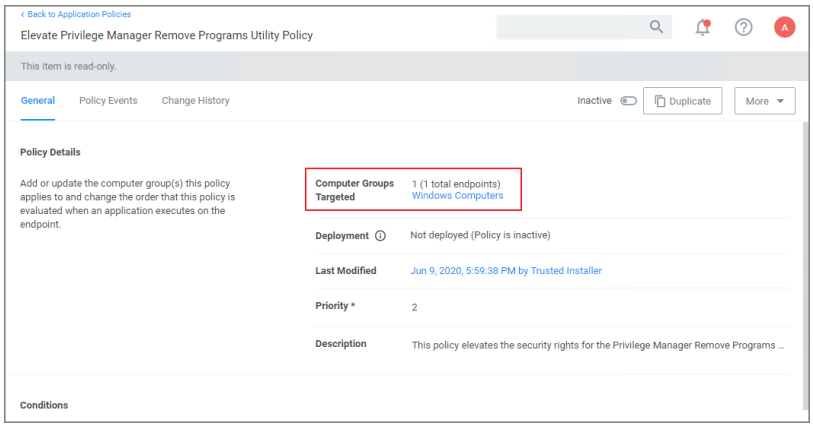


These OUs are what you can select using the "Group" option, for "List Type", when building a target.

Note: Changes made in AD are not immediately reflected in Privilege Manager. Setup scheduled tasks to periodically import changes. The operation can be long-running for large domains, so be careful about the frequency with which you schedule the import.

Assigning Policies to Targets

To assign a policy to your target or better to add your target to a policy, find the policy on the Policies page and edit the **Policy Details**. Use the **Add** and **Edit** options to modify your policy.



Refer to the "Application Policies" on page 230 to review details about Policy Administration.

Collections

A collection is a predefined list of computers. A collection is often meant to act as a filter and hence is also sometimes referred to as a filter.

Collections are typically defined by an SQL query that returns a list of computer IDs or other resource IDs.

Built-in collections are available in Privilege Manager, for example, "All x64 Windows Computers" and "Domain Controllers."

User defined collections are possible but typically expected to be created by Privilege Manager professional services, on behalf of a user, rather than directly by a user. Users are encouraged to define custom targets using existing (built-in) collections, groups, and fixed lists rather than creating new collections.

Filter Types and Descriptions

There are different types of filters for different operating systems and applicable functional areas. When creating a new filter,

- the **Platform** drop-down offers a choice of macOS, Windows, and Unix/Linux.
  - Unix/Linux
  - macOS
  - Windows
- when Windows or macOS is selected as a platform, the **Filter Type** drop-down gives a list of options based on that platform selection:
  - Application Filters
  - File Filters
  - Inventory Filters

These are loose groupings that signify a few different approaches to the filtering method or targets.

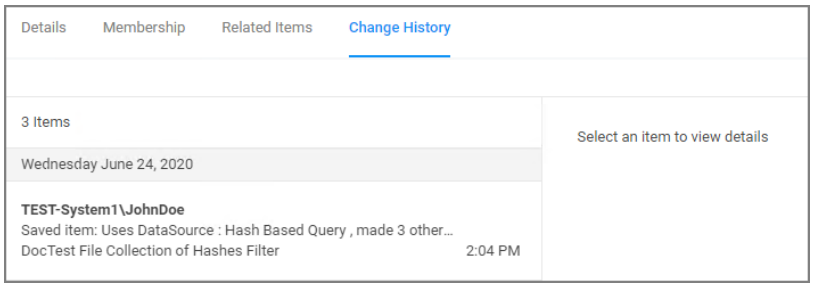
Common Filter Characteristics

Each filter has a Details area that contains the filter name, description, and platform association. These details are usually specified when you create the filter, either by choosing **Create Filter**, editing an existing filter, or duplicating an existing filter.

Those characteristics are used for searches or filtering and allow users to easily find existing filters.

Filter Change History

Each filter has a **Change History** tab, where audit information can be reviewed from the time the filter was created in the system.

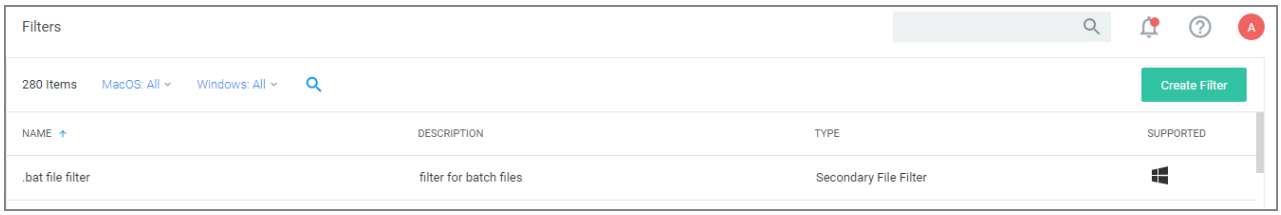


Refer to Change History to learn more about drilling down into the change history of resources and the report.

How to Search for Filters

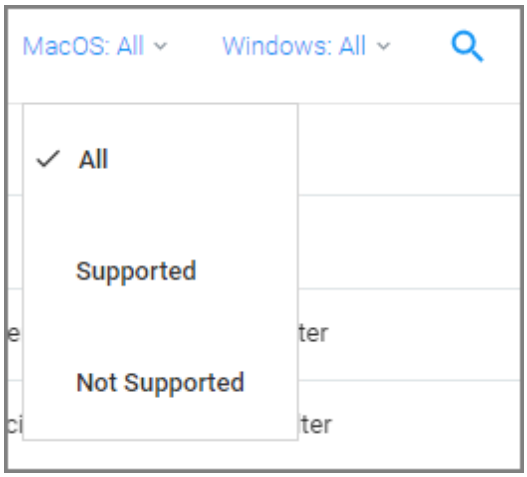
All out-of-the-box filters can be searched, duplicated, and then customized to be used in policies.

1. Navigate to **Admin | Filters**.

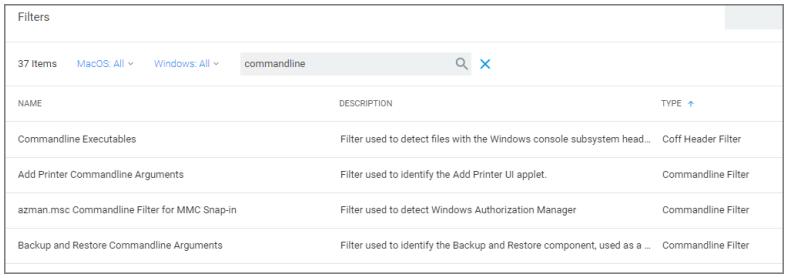


The list of all filters is sortable by Name (default), Description, Type, and OS Support.

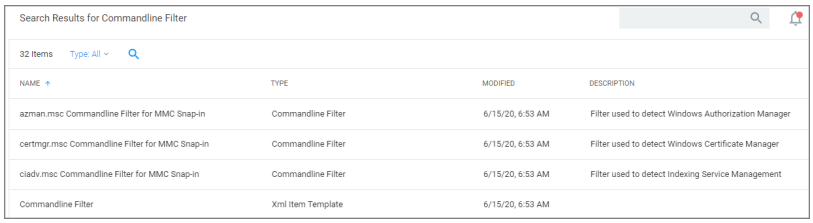
You may limit your list output, by changing from the default **All** or Supported selection for macOS or Windows to Not Supported.



2. Using the search option next to the OS drop-down, lets you search the list contents based on the column the contents is sorted by. So if your list is sorted by **Name**, but you are looking for all commandline filter types you have in the system, sort your list by **Type** first.
3. Then click **Search** and enter a search term, for this example *commandline*.



You can also use the search option on the top-right from any page of your Privilege Manager console and get the a list of commandline filters returned. If you use this search option, the search field does not retain your search term. The results are based on the search term matching the Name and/or Type, so the list will contain more items than searching based on column selection.



The columns returned for this search are sorted by Name (default), Type, Modified Date, and Description.

Application Filters

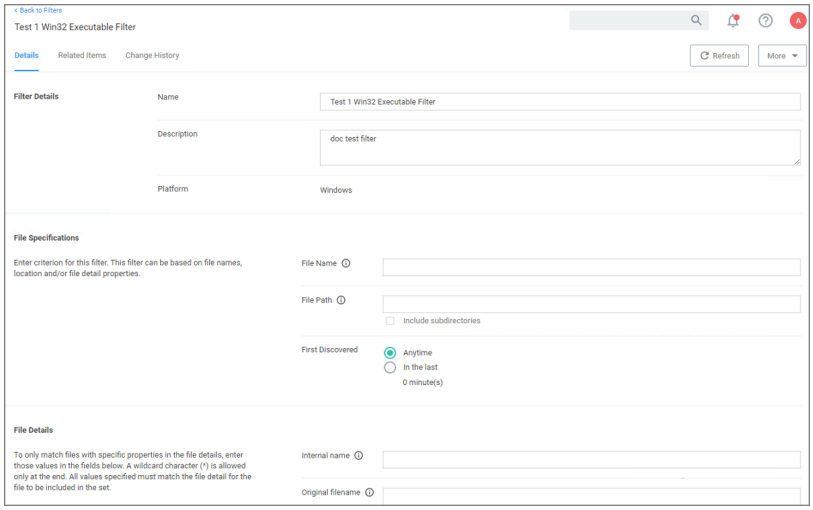
These generally target specific executables or things about the environment. These types of filters can be used to limit policies to a certain time of day, the parent process of an application, the security rating of an application, or the user or group running the process.

The following Application Filter type filter topics are available:

- Blank Wind32 Executable Filter
- Commandline Filter
- Download Source Filter
- Environment Filter
- Network Location Filter
- Parent Process Filter
- Secondary File Filter
- Security Rating Filter
- Signed File Filter
- Time Of Day Filter
- User Context Filter
- User Context Filter via SID

Blank Win32 Executable Filter

Identifies specific application files by specifications like name, path, and when first discovered.



Parameters

Win32 Executable filters have two sets of parameters:

- **File Specifications**, such as
  - File Name
  - File Path with option to include subdirectories
  - First Discovered, which can specified as "Anytime" or "In the last" either Minutes, Hours, Days, or Weeks.
- **File Details** (common attributes), such as

- Internal name
- Original filename
- File version
- Product name
- Product version
- Company name
- Copyright (version 10.7 and up)

Examples

Used to target specific applications, for example allowing acrobat.exe or notepad++.msi to be used on endpoints.

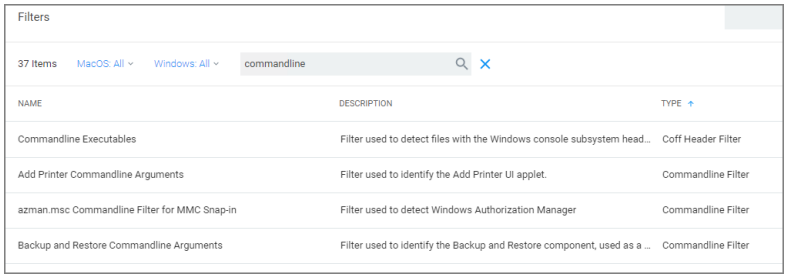
Commandline Filter

These filters will perform an exact, partial or regex match on the commandline of the process. Privilege Manager comes with default commandline filter types, which are all read-only, but can be copied to be customized.

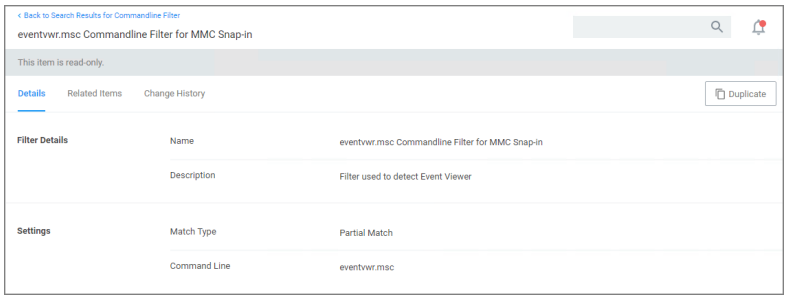
This filter is available for both Windows and macOS systems.

Search for Commandline Filters

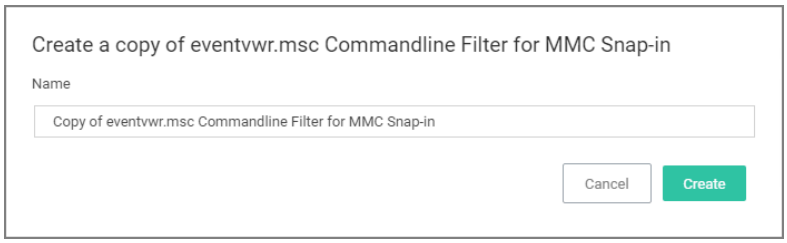
1. Navigate to **Admin | Filters**.
2. In the search field for the **Type** column enter commandline.



3. Select a filter to view its details and/or use **Duplicate** to customize the filter.

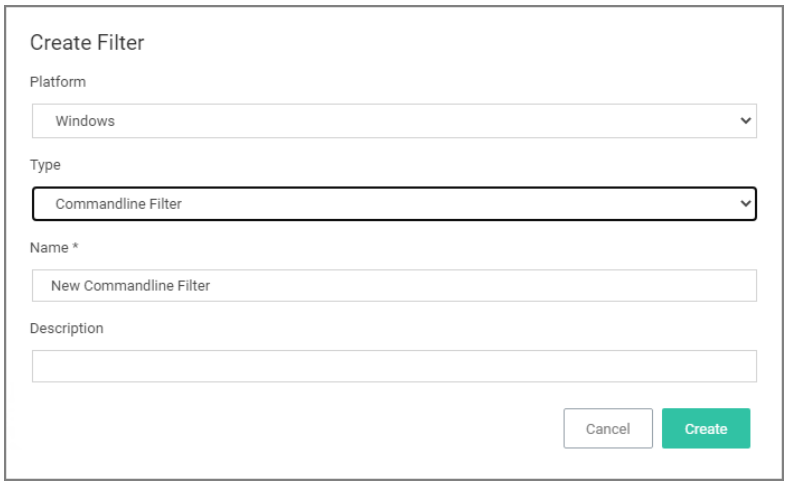


If you Duplicate (make a copy of an existing) filter, "rename" the filter and click **Create**.

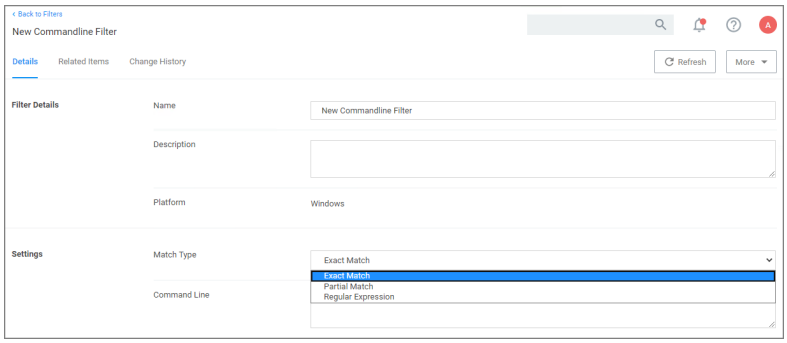


Create a New Commandline Type Filter

1. Navigate to **Admin | Filters**.
2. Click **Create Filter**.
3. On the New Filter page, select the platform. For this example, select **Windows**.
4. From the **Filter Type** drop-down select **Commandline Filter**.
5. Enter a name and description and click **Create**.



6. Customize the newly created filter.



a. Under **Settings**,
   i. Set the **Match Type**. This can be either an exact or partial match or specified as a regular expression.
   ii. Enter the commandline to match.

7. Click **Save Changes**.

Parameters

Commandline Filters have one section to set the parameters for the filter.

The **Match Type** gives you the options:

- Exact Match
- Partial Match
- Regular expression

Command Line:

- This is the section where you enter in the given command parameters to pull up the file or action.

> **Note:** You can turn on agent trace logging to view the command line being evaluated against the Regex expression to troubleshoot any issues with the filter matching.

Examples

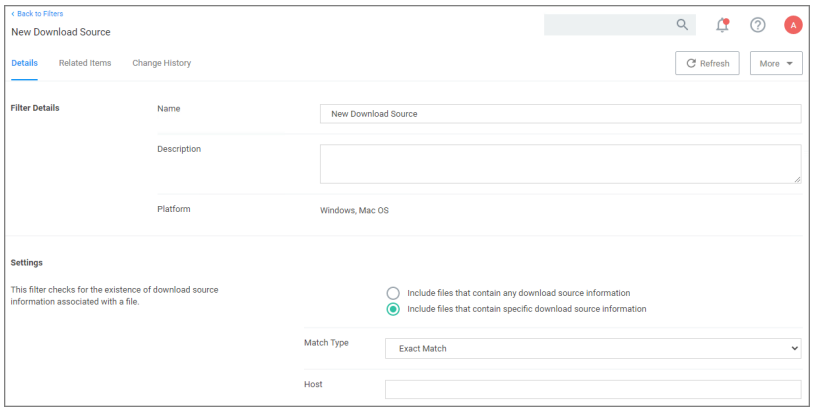
A commandline filter examines the commandline (excluding the primary executable) and applies a pattern match (Exact, Partial or Regular Expression).

For example allowing /FlushDNS as a command for IPConfig.

Download Source Filter

The filter checks where a file is being downloaded from. This filter allows you to identify specific download sources, and allows the ability to allow list sources you trust or block sources you don't. *No out-of-box filters exist in Privilege Manager for this type*.

This filter is available for both Windows and macOS systems.



Parameters

The filter checks for the existence of download source information associated with a file.

Settings:

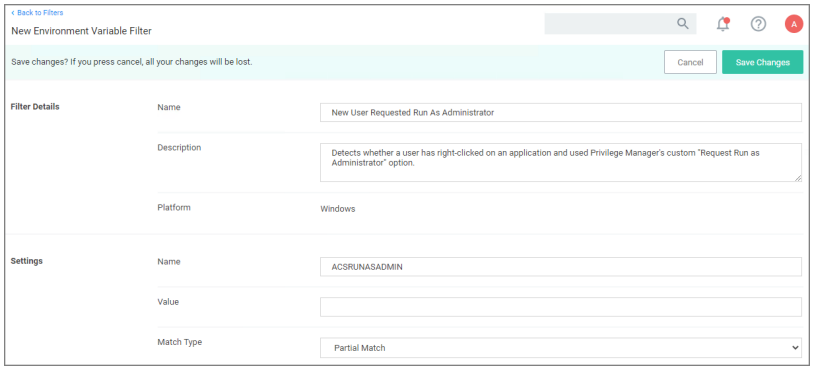
- Include files that contain any download source information
- Include files that contain specific download source information
- Match type
- Host

Examples

This filter would allow you to control what download sources should be allowed or blocked.

Environment Variable Filter

This type of filter can target environment variables of a process that is started.



Parameters

- Name
- Value

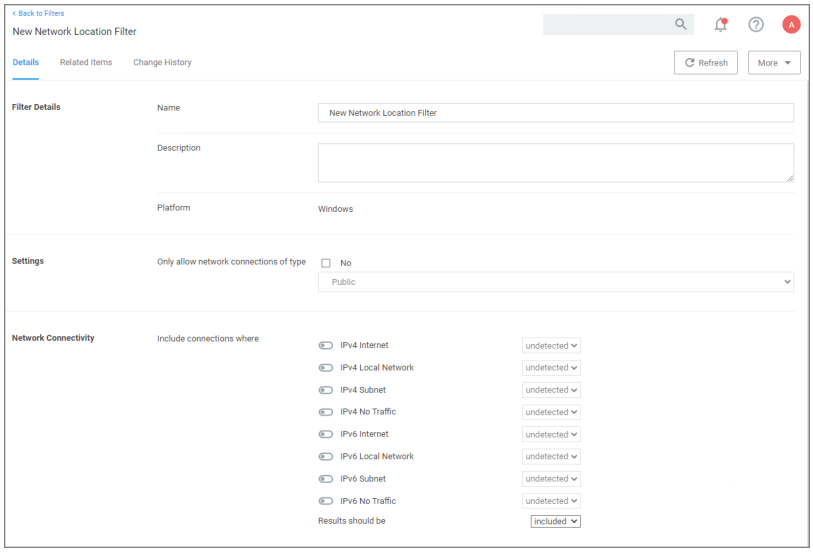
- Match Type:
  - Exact Match
  - Partial Match
  - Regular expression

Examples

A environment variable filter type detects whether a user has right clicked on an application and used Privilege Manager's custom *Request Run as Administrator* option.

Network Location Filter

This type of filter identifies a computer's connection to specific networks like public, private, or unclassified networks.



Parameters

You can adjust the following setting options for Network Location filters:

- **Only allow network connections of type**:
  - Public
  - Private
  - Domain
- **Network Connectivity**:
  - IPv4 and IPv6 options for connectivity
- **Results should be**:
  - Included or excluded

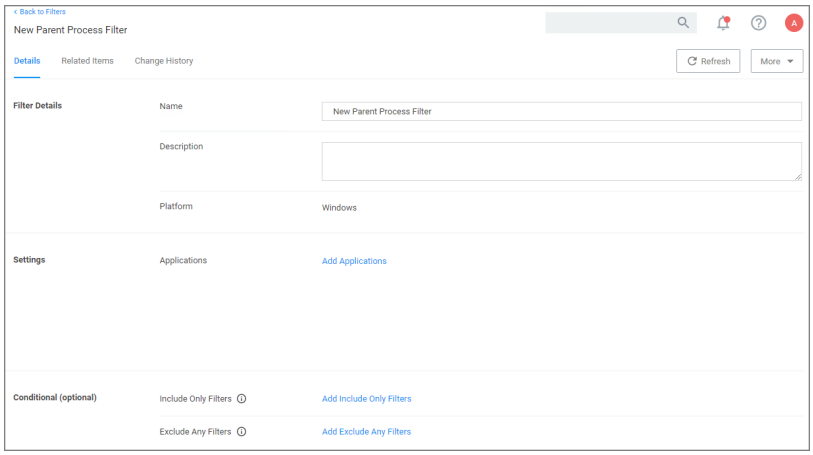
Examples

Some examples of this filter can be set to detect:

- when the computer is not attached to a network
- when the computer is attached to a network classified as public
- when the computer is attached to a network classified as domain

Parent Process Filter

This type of filter can identify parent processes of certain executables.



This filter is available for both Windows and macOS systems.

Parameters

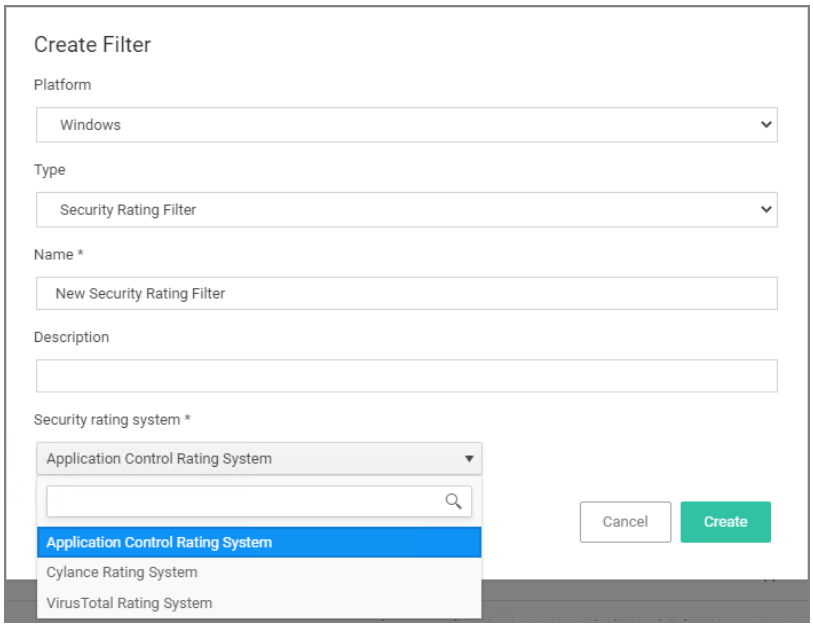
- Applications
- Conditions
- Include only filters
- Exclude any filters

Examples

This filter is used to detect when a user attempts to copy a file using the Privilege Manager copy helper.

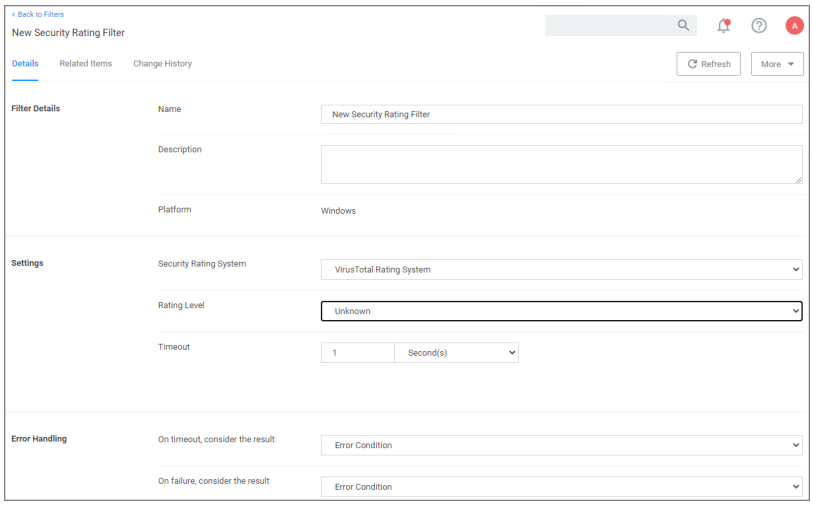
Security Rating Filter

If you have integrated Privilege Manager with a Reputation Checking provider like VirusTotal, these filters allow you to look up a rating for a file or application (is it good, bad, suspect/suspicious, or unknown).



This filter is available for both Windows and macOS systems.

Parameters



The parameters for the Security Rating Filter would include the following:

- Security Rating System
  - Application Control Rating System
  - Cylance Rating System
  - VirusTotal Rating System
- Rating level

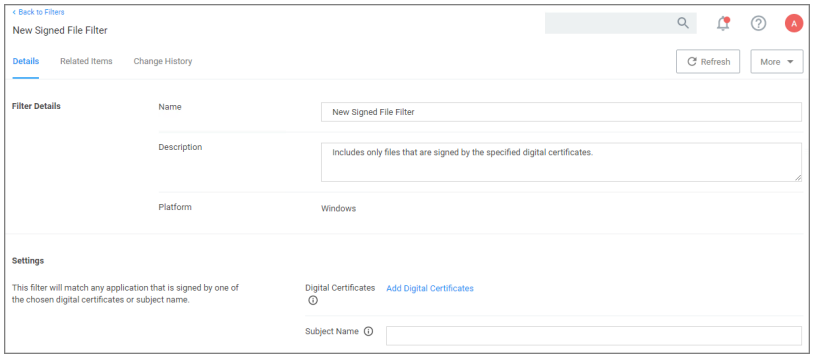
  - Unknown
  - Clean
  - Suspect
  - Bad
- Timeout, can be specified in seconds or milliseconds
- Error Handling
  - On timeout, consider the result
    - Matched
    - Note Matched
    - Error Condition
  - On Failure, consider the result
    - Matched
    - Note Matched
    - Error Condition

Examples

The example above displays how to create a security rating filter after integrating Privilege Manager with VirusTotal.

Signed File Filter

This filter allows you to associate one or more Digital Certificate(s) that are trusted and verify that an application or file is signed by one of those certificates. *No out-of-box filters exist in Privilege Manager for this type*.



These filters can be used in several of the following ways:

- A target for ACS policies
- A parameter to prevent spoofing

Signed Application filters identify applications based on their digital certificates.

This filter is available for both Windows and macOS systems.

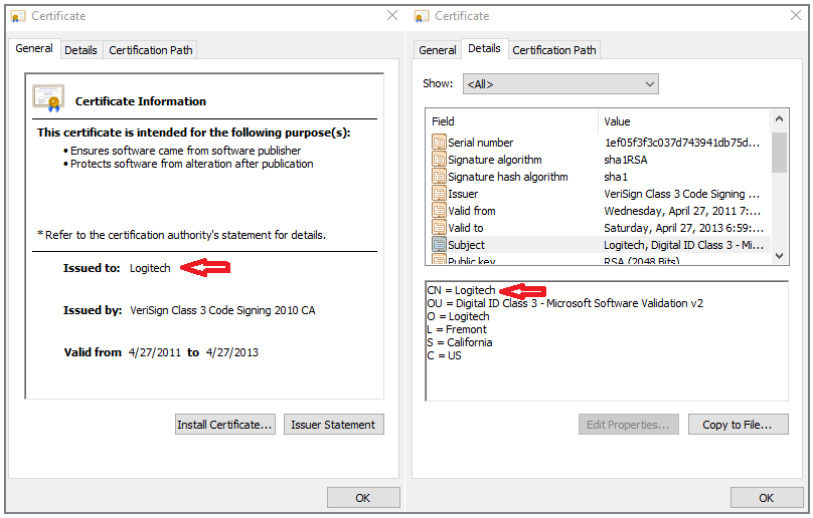
Parameters

Under Settings users:

- add one or more digital certificates, which are discovered via inventory.
- enter a Subject Name (version **10.7 and up**). If Subject Name is specified, the digital certificates above will be ignored. The following three match types are supported:
  - The * character can be pre- or post- appended to a string to perform a begins with or ends with match (i.e. `Microsoft*`).
  - Lower-case RegEx is also supported and must be surrounded with parenthesis. (i.e. `(micro.*)`)
  - Setting the subject name to * will match any file signed with a valid certificate. (**Not recommended by Thycotic**)

Subject Name

This filter matches on the common name (CN=) data of the certificate as the Subject Name. Make sure to specify the right string, for example for the following certificate the filter Subject Name field would contain Logitech.



If the common name contains quotes on the certificate, those quotes should NOT be used in the Subject Name field.

Examples

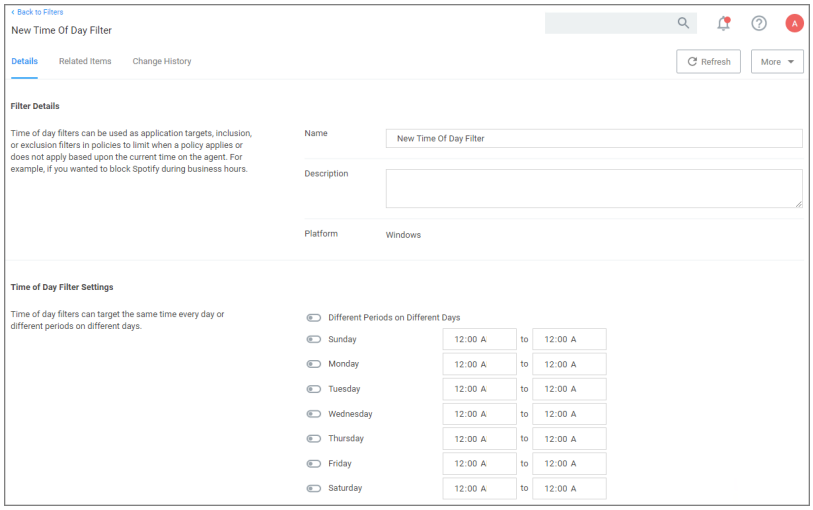
Adobe (TM) requires several certificates that are used to sign applications.

Because of this, you may want all applications signed by Adobe to allow listed, so that a signed application filter targeting Adobe Certificates allows all applications signed by Adobe to run.

Targeting the latest Adobe Flash Installer via a Win32 Executable filter and then using the signed application filter ensures that the application really is the adobe flash installer. The Signed Application Filter works as a validation filter for applications.

Time of Day Filter

This type of filter exists to create policy parameters for specific time frames.



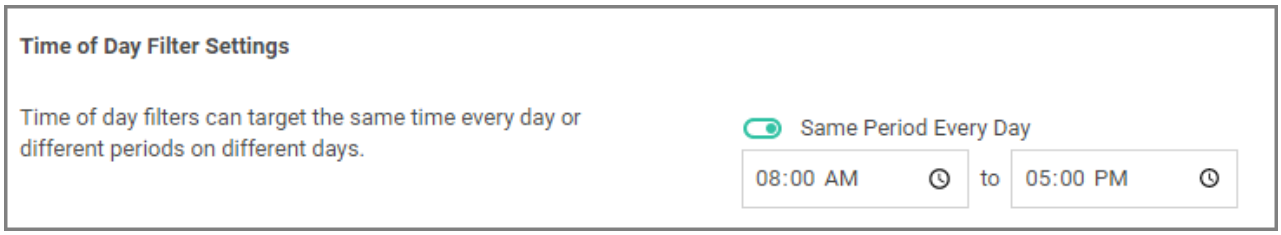
This filter is available for all supported platforms.

Parameters

The time of day filter has two different settings to allow you to set time and day allowances.

Flip the switch to toggle between these option:

- **Different Periods on Different Days** (default). When set to Different Periods on Different Days, the page also shows switches to turn on the time of day settings for the specific day of the week. By default no periods are enabled.
- **Same Period Every Day**, when turned ON only one period entry option is available



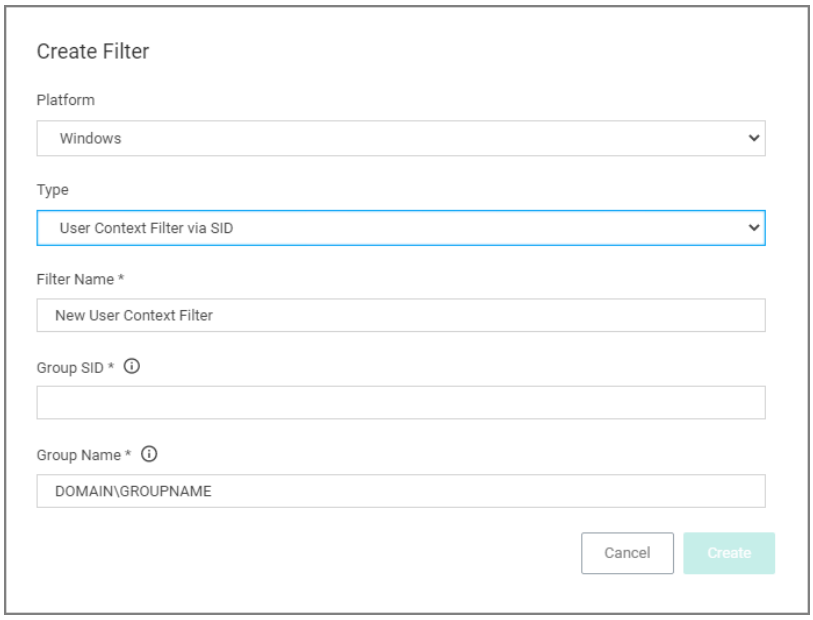
Save the changes after any customization.

Examples

You can use the time of day filter in a policy to only pickup specific times or days of the week.

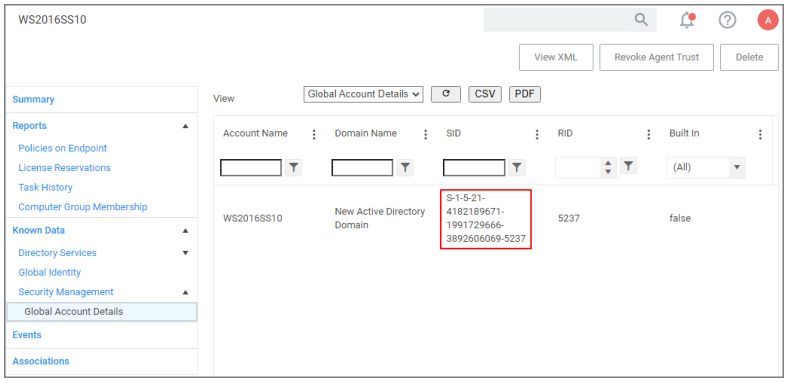
Using User Context Filters via SID

For Privilege Manager Cloud, the **User Context Filter via SID** can be used if (Azure) AD synchronization has not been set up but the SID of the group is known. When creating the filter,

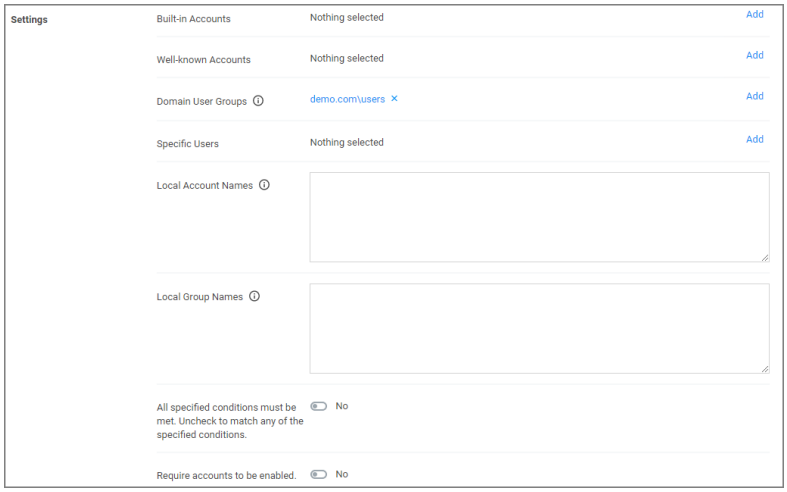


enter the

- **Group SID**, which you can find under the Global Account Details for a given resource:



- **Group Name**, to name the group if it does not exist.



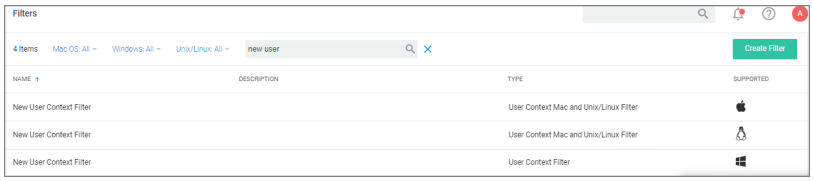
If the Group SID and Group Name are not known for a resource, Delinea recommends customers use the User Context Filter as described here.

Using User Context Filters

User Context Filters are used in a policy as either an

- inclusion filter, to specify that the policy only applies to users in a specific AD Group.
- exclusion filter, to specify that the policy applies to everyone except the users in a specific AD Group.

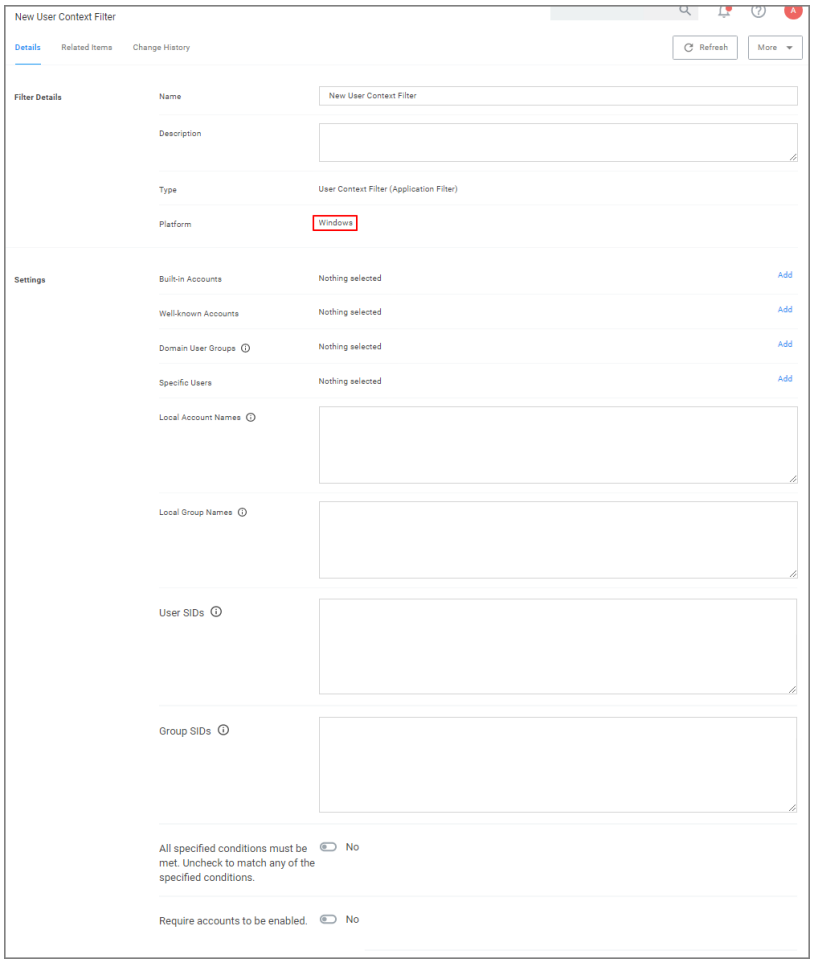
The User Context Filters are part of the Application Filter templates listed for Windows, macOS, and Unix/Linux systems, once created the OS type is referenced:



This filter is available for all supported operating systems, with a couple of minor differences.

Windows

On Windows 10 endpoints, the filter ensures that Azure AD security groups can be targeted within Windows-based User Context Filters computers that are **only** joined to Azure AD. The User Context by User or Group SID allows the user to target an account (user or group) even if that account has not yet been inventoried in the server.



For Privilege Manager on-premises, the **User Context Filter** can be used after the Active Directory synchronization completes. When creating and editing the filter, add any

- Built-in Accounts,
- Well-known Accounts, and/or
- Domain User Groups, for which you may need to run the Active Directory sync task to update available users and groups, or
- Specific Users,
- Local Account Names,
- Local Group Names,
- User SIDs,
- Group SIDs

to specifically select user and group context.

Then set the **All specified conditions must be met** switch to **Yes**, if **ALL** conditions must be met. Leave the switch set to **No** to match **ANY**.

You can also specify if accounts must be enabled to be targeted. This is an important checkbox to set if specific users have been added.

Refer to Using User Context Filters via SID to set up a User Context Filter via SID, if Azure AD synchronization has not yet happeded, but the Group SID is known.

macOS

On macOS endpoints, the filter can be set-up to target Domain User Groups when endpoints are integrated with NoMAD.

Refer to Leveraging the User Context Filter for NoMAD for macOS specifics of the User Context Filter.

Unix/Linux

Refer to User Context Filter under the Unix/Linux Filter section for Unix/Linux specifics of the User Context Filter.

Using Secondary File Filters

This topic explains how to create policies for applications that trigger file executions. Implementing a policy to filter on a file type, which is used by another executable, is done by setting a **Secondary File Filter**. The Secondary File Filter is available for both Windows and macOS systems.

The following topics show the steps to create policies and include filters that enforce actions on endpoints when batch files, PowerShell scripts, or Microsoft Installer files execute. Any type of executer can be specified and policed this way.

In general, the steps are similar for the different file types to be policed.

Via File Inventory

- With Learning Mode enabled, you use the File Inventory to discover new resources.
- Select a discovered resource and use **Create Filter**.
- On the Manage Application modal select which specifications to match.
- Use **Create and Add to Policy** option.

Via Policy Wizard

- You create a controlling policy via the Wizard.
- On the **What do you want to target step?** you can select an existing filter, upload a file (recommended for .msi/.exe applications), or use an already inventoried file.
- Policy Wizard builds the policy and after you name and create it, you can further customize all the details. The Policy wizard automatically adds the correct application targets, inclusions an/or exclusions.

Examples

- Best Practices
- Targeting script file execution, like .bat and .ps1
- Targeting installer/executables execution, like .msi and .exe

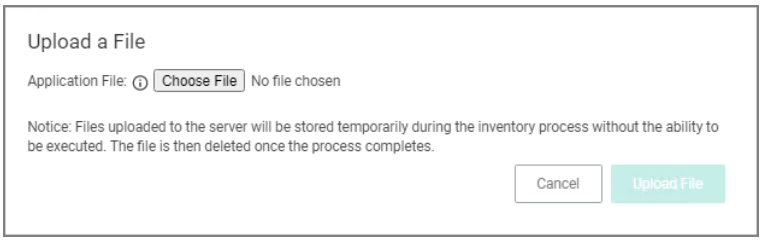
Script Execution File Example

In this example we are creating a policy to deny running a batch or ps1 file, which the policy targets through a secondary file filter.

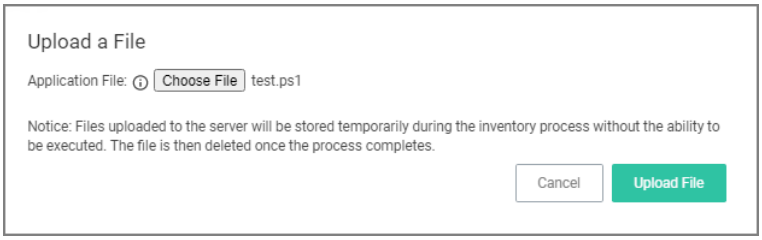
This example is for a Windows endpoint, but the policy can be created in the same way for a macOS system.

Creating the Policy

1. Navigate to **Computer Groups | Windows Computers**.
2. Select **Application Policies**.
3. Click **Create Policy**.
4. In the policy wizard select **Controlling**, click **Next Step**.
5. In the policy wizard select **Block**, click **Next Step**.
6. In the policy wizard select **Notify and Block**, click **Next Step**.
7. In the policy wizard select **Script**, click **Next Step**.
8. In the policy wizard select **File Upload**.
   a. On the Upload a File modal, Click **Choose File**.



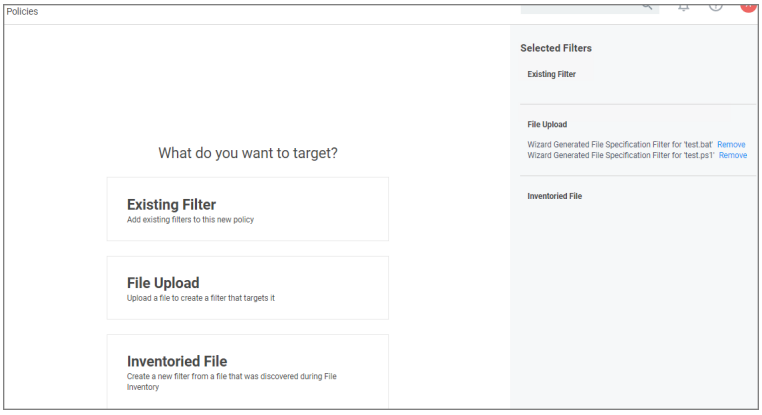
   b. Select the file(s) you wish to be targeted. For this example we are first uploading a test.bat and then test.ps1 file. You need to run through the upload and manage application steps twice, once for each file you are uploading.



   c. Click **Upload File**.
   d. On the Manage Application dialog, check **File Name**.

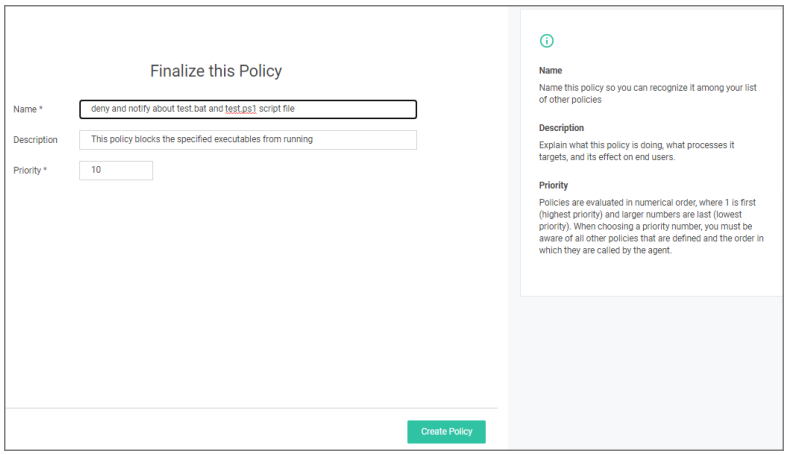
Select more details like the File Path or the Hash, if you want to make this policy more specific.

e. Click **Create Filter**.



f. Click **Next Step**.

9. On the Finalize the Policy page, enter a name for your new policy. The policy will be created with a default priority of 10, since it is a deny and notify policy.



10. Click **Create Policy**.

General | Policy Events | Change History

Inactive | Refresh | More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted	1 (1 total endpoints) Windows Computers ×	Add
Deployment	Not deployed (Policy is inactive)	
Last Modified	Jun 30, 2020, 3:47:34 PM by WIN-E6GKPM7J7TF\Administrator	
Priority *	10	
Description	This policy blocks the specified executables from running	

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc.
Filters

Applications Targeted	Command Processor (cmd.exe) Powershell (powershell.exe) Scripting Host (cscript.exe) Scripting Host (wscript.exe)	Edit
Inclusions	Scripts for 'deny and notify about test.bat and test.ps1 script file'	Edit
Exclusions	Add Exclusions	

Actions

Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy
Actions

Actions	Deny Execute Deny Execute Message	Edit
Child Actions	Add Child Actions	
Audit Policy Events	Record all activity detected by this policy in Policy Events	

Show Advanced

The policy wizard added based on the selected file uploads and the file inventory that was executed 4 types of application targets:

- Command Processor (cmd.exe)
- Powershell (powershell.exe)
- Scripting Host (cscript.exe)
- Scripting Host (wscript.exe)

A secondary file filter was added under Inclusions, identifying two specific file filters for the test.bat and test.ps1 files.

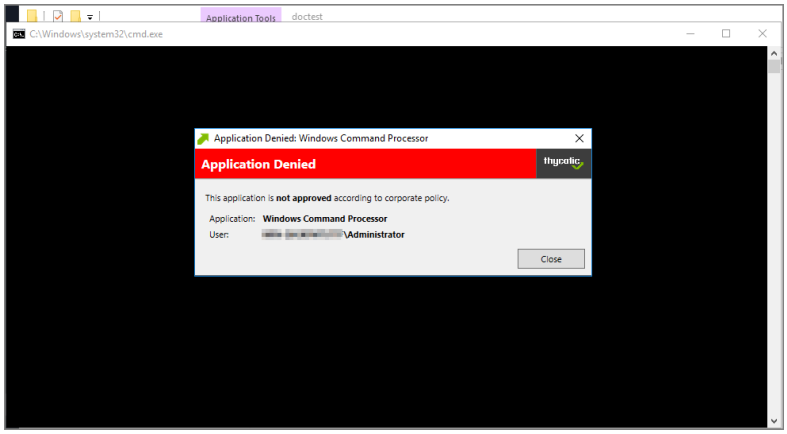
Verifying the Policy Works

1. Add a test.bat file with a simple Hello World command to your system.
   a. Create a new text file and add

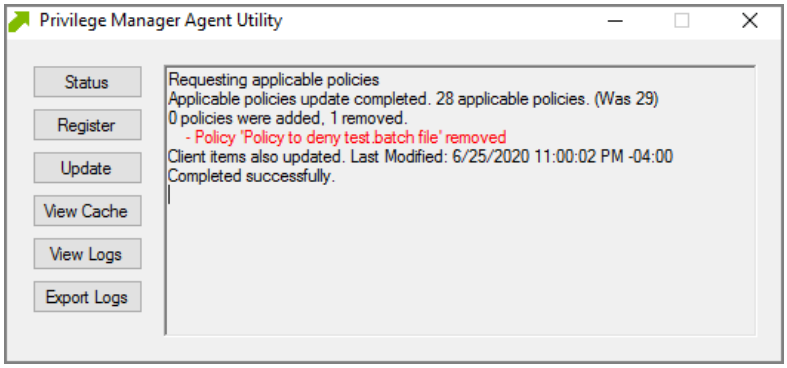
```
ECHO OFF
ECHO Hello WorldPAUSE
```

   b. Save the file as test.bat.
2. With your policy set to **active**, double-click the test.bat file.

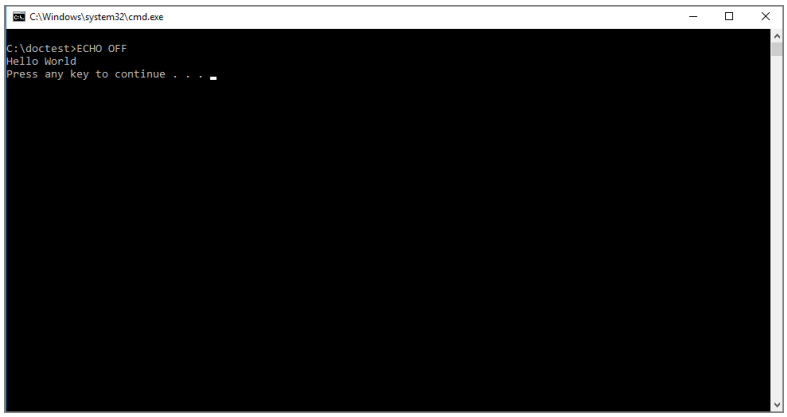
The policy triggers the specified message action:



3. With your policy set to **inactive**, verify via Agent Utility that the update was received and the policy was removed:



4. Double-click the test.bat file.



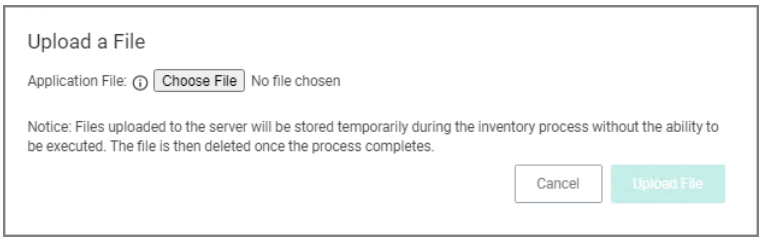
The batch file is executed and Hello World is printed to the cmd.exe output window.

Executables File Example

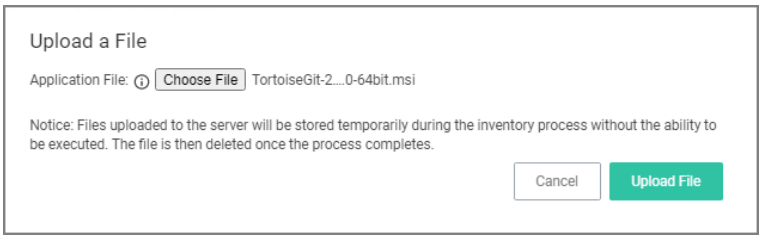
In this example we are creating a policy to deny running .msi files.

Creating the Policy

1. Navigate to **Computer Groups | Windows Computers**.
2. Select **Application Policies**.
3. Click **Create Policy**.
4. In the policy wizard select **Controlling**, click **Next Step**.
5. In the policy wizard select **Block**, click **Next Step**.
6. In the policy wizard select **Notify and Block**, click **Next Step**.
7. In the policy wizard select **Installer Packages**, click **Next Step**.
8. In the policy wizard select **File Upload**.
   a. On the Upload a File modal, Click **Choose File**.

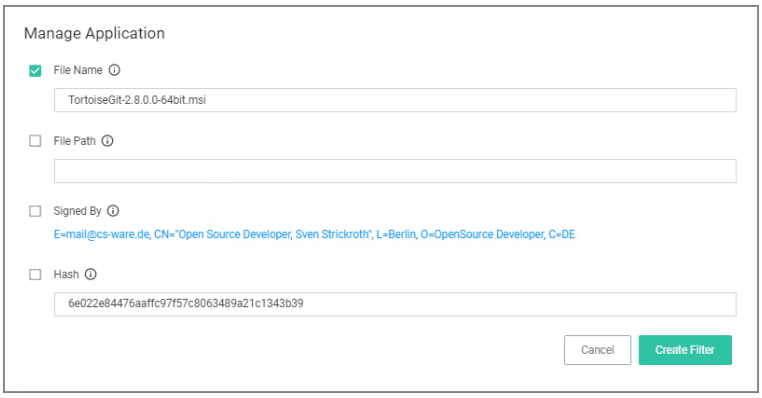


   b. Select the file(s) you wish to be targeted. For this example we are selecting a TortoiseGit installer package.



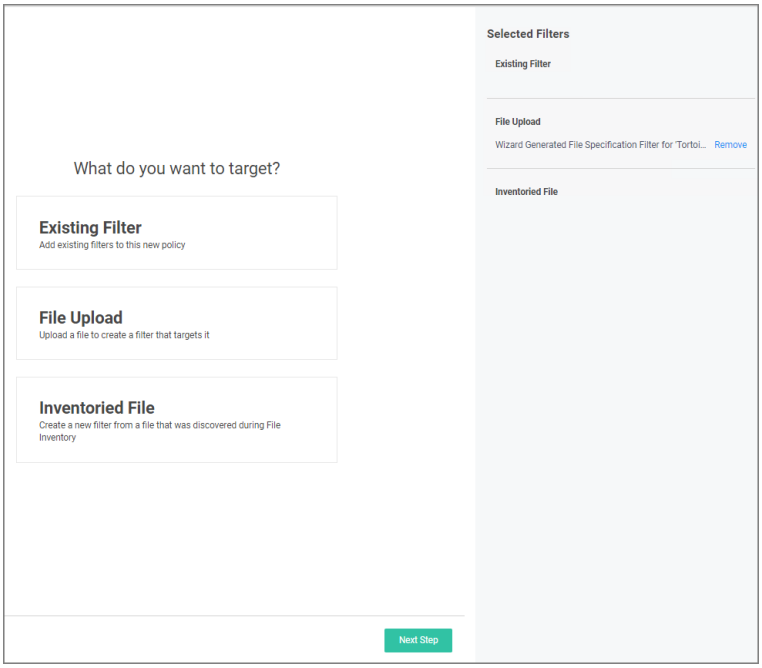
c. Click **Upload File**.

d. On the Manage Application dialog, check **File Name**.



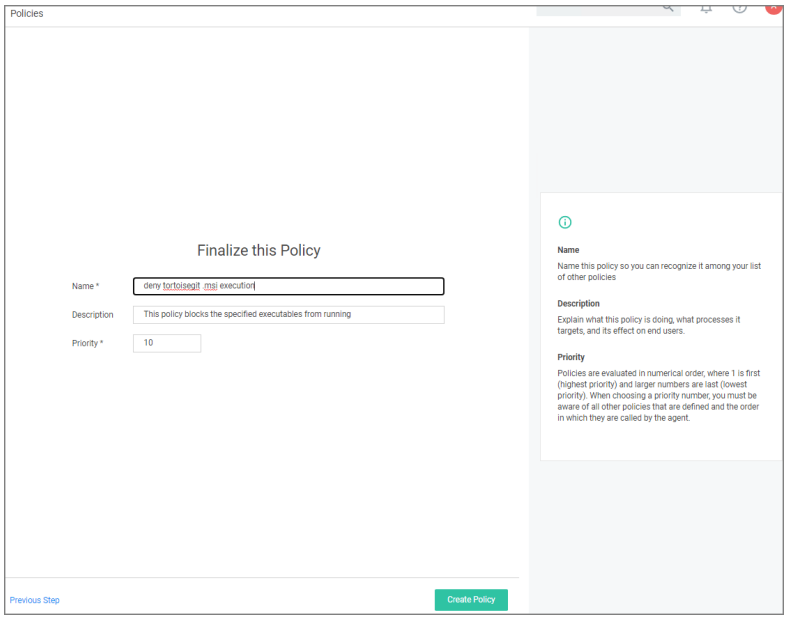
Select more details like the File Path or the Hash, if you want to make this policy more specific.

e. Click **Create Filter**.

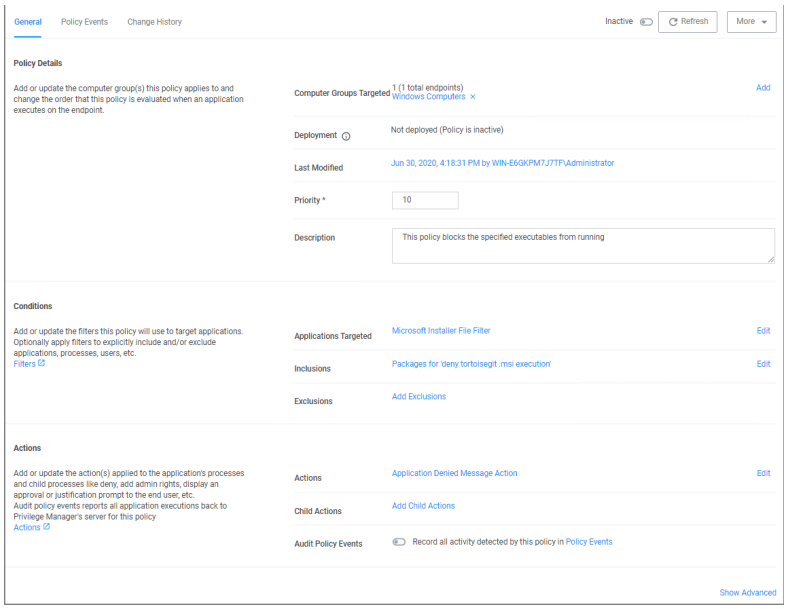


f. Click **Next Step**.

9. On the Finalize the Policy page, enter a name for your new policy. The policy will be created with a default priority of 10, since it is a deny and notify policy.



10. Click **Create Policy**.



The policy wizard added based on the selected file upload and the file inventory that was executed and application target of Microsoft Installer Files.

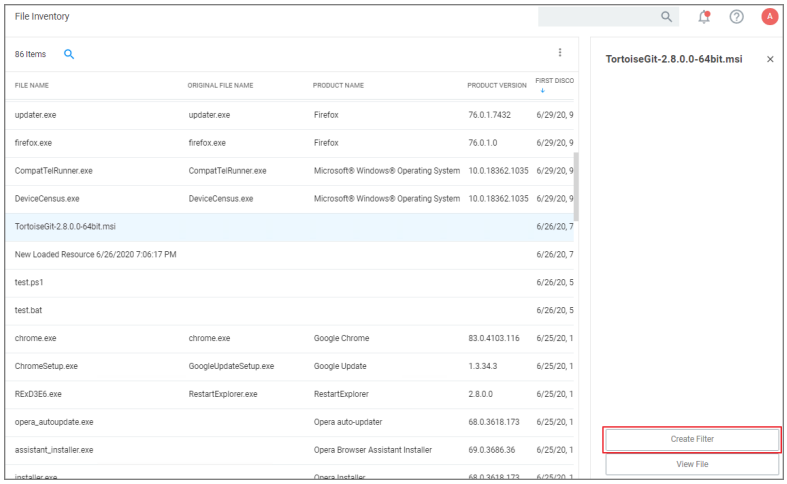
A secondary file filter was added under Inclusions, identifying a specific file filter for the tortoisegit.msi execution.

Best Practice: Using a Secondary File Filter

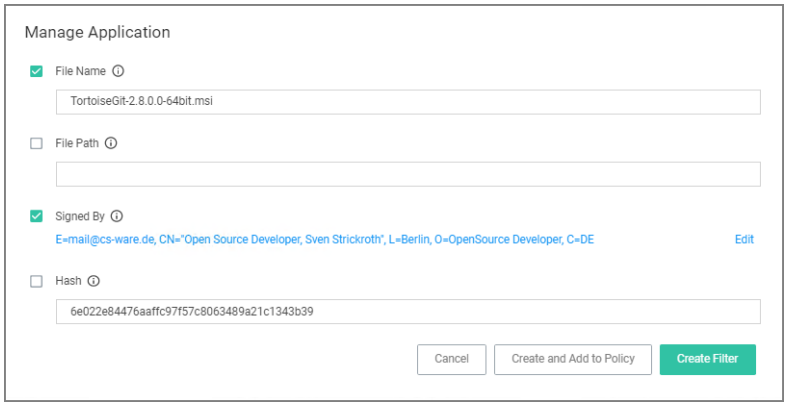
Using File Inventory

As a best practice you create an elevate policy with a priority of X (for example 85) to elevate or allow specific scripts or files to run. Then you add a policy with a priority of X+1 to deny any other execution of the command processor, PowerShell, or Microsoft installer files. For this example .msi is used.

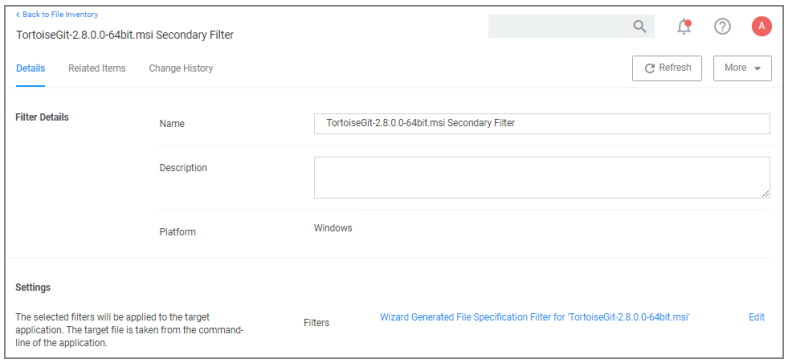
1. In the Privilege Manager Console under **Computer Groups** navigate to **File Inventory**.
2. From the list of discovered resources, we are selecting our example TortoiseGit.



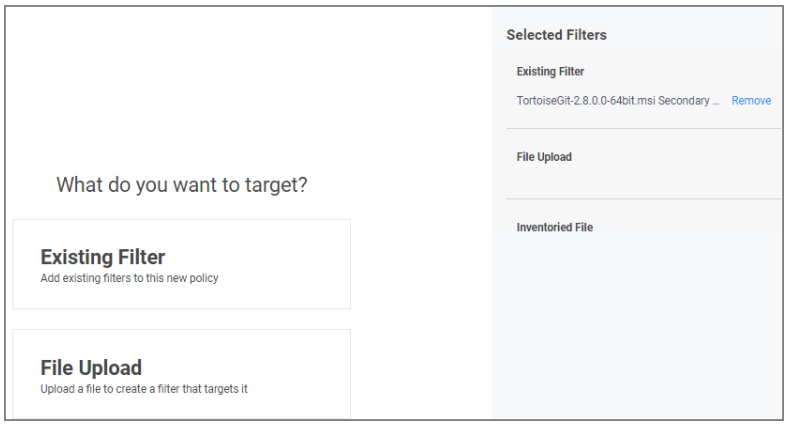
3. Click **Create Filter**.
4. On the Manage Application page, check the **File Name** and **Signed By** checkboxes.



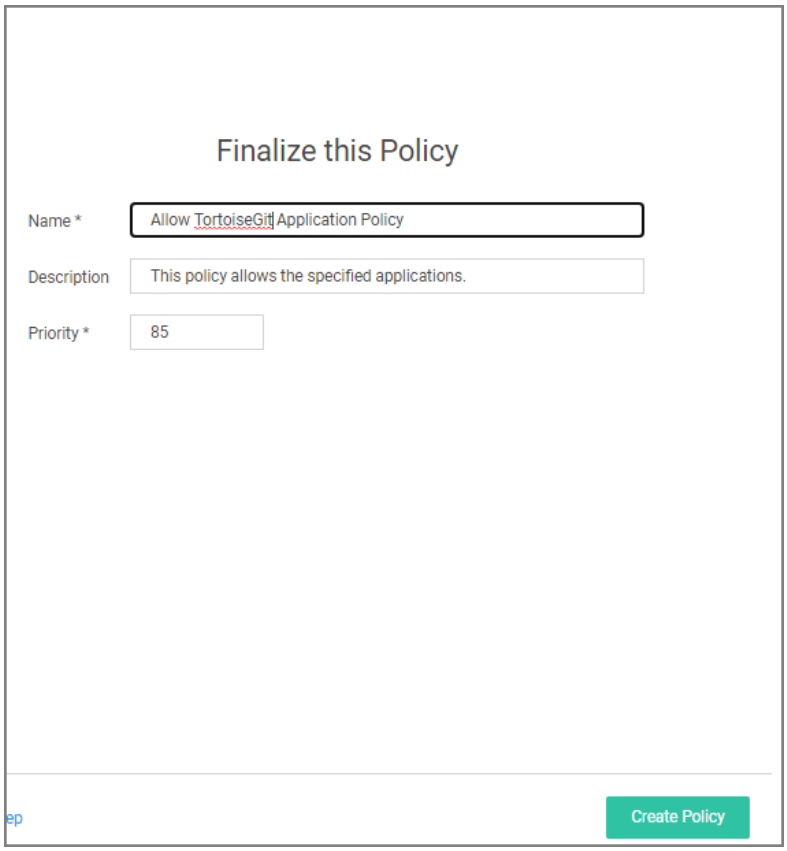
5. Click **Create Filter**.



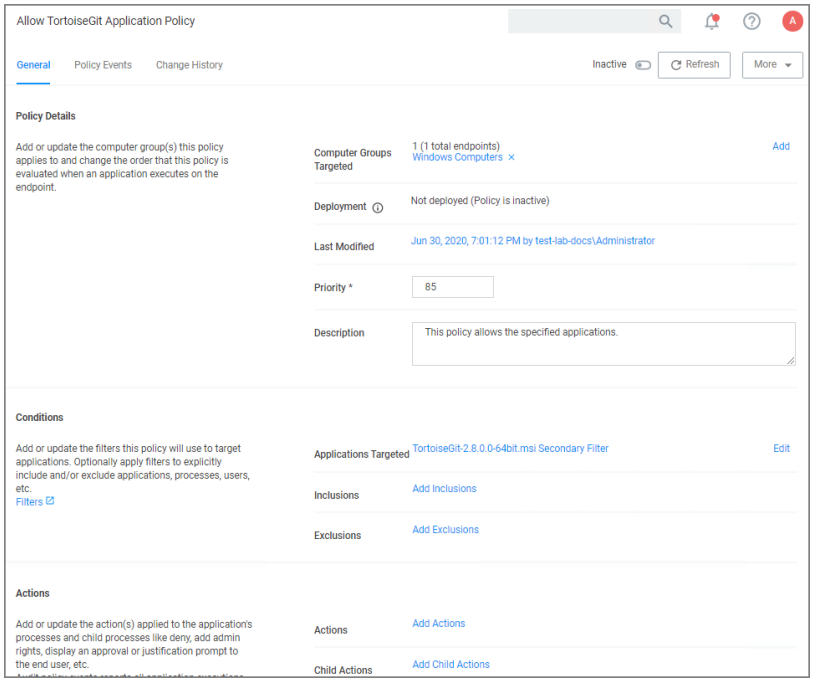
6. Navigate to **Computer Groups | Windows Computers**.
7. Select **Application Policies**.
8. Click **Create Policy**.
9. In the policy wizard select **Controlling**, click **Next Step**.
10. In the policy wizard select **Allow**, click **Next Step**.
11. In the policy wizard select **Specific Applications**, click **Next Step**.
12. In the policy wizard select **Existing Filter**, click **Next Step**.
    a. Search for and add the secondary file filter created from the file inventory above.
    b. Click **Update**.
13. On the policy wizard page that now lists the existing filter, click **Next Step**.



14. Name the policy and click **Create Policy**.



The policy wizard added based on the selected filter the application target to allow the TortoiseGit application.



File Filters

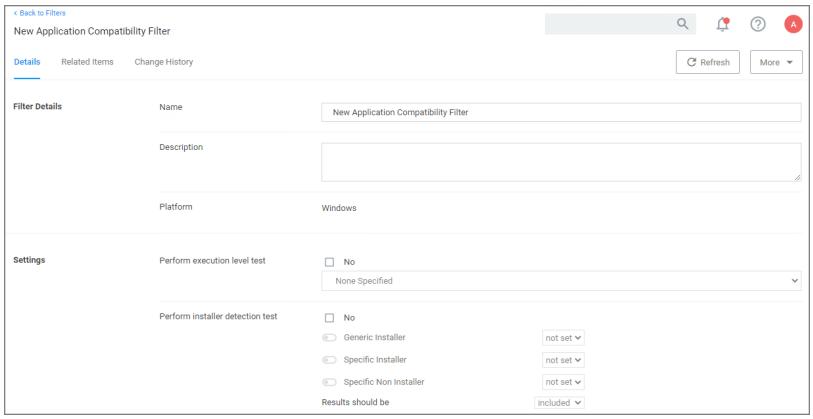
These target specific file information. File Filters can be used to target the file owner of the application, the type of file, the application manifest of the file, or whether the application is present in the signed security catalog (Operating System Files).

The following File Filter type filter topics are available:

- Application Compatibility Filter
- Application Manifest Filter
- File Collection Security Catalog Filter
- File Existence Filter
- File Owner Filter
- File Specification Filter
- File Type Filter
- Internet Zone Filter
- Security Catalog Filter

Application Compatibility Filter

This type of filter identifies the rights or permissions that an application requires to run.



Parameters

By default **Perform execution level test** is set to no, if you change this to Yes, you can specify:

- As Invoker
- Highest Available
- Require Administrator

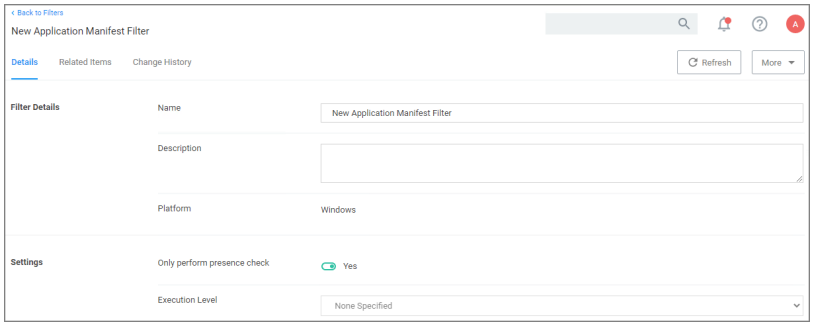
By default **Perform installer detection test** is set to no, if you change this to Yes, you can specify:

- Generic Installer to be set or not set.
- Specific Installer to be set or not set.
- Specific Non Installer to be set or not set.
- if the Results should be included or excluded.

Remember to **Save Changes** after any customization.

Application Manifest Filter ("Manifest Filter")

Applications that declare specific rights required via a manifest, such as applications that need administrative privileges.



Parameters

By default **Only perform presence check** is set to Yes, if you change this to No, you can specify the **Execution Level** as either:

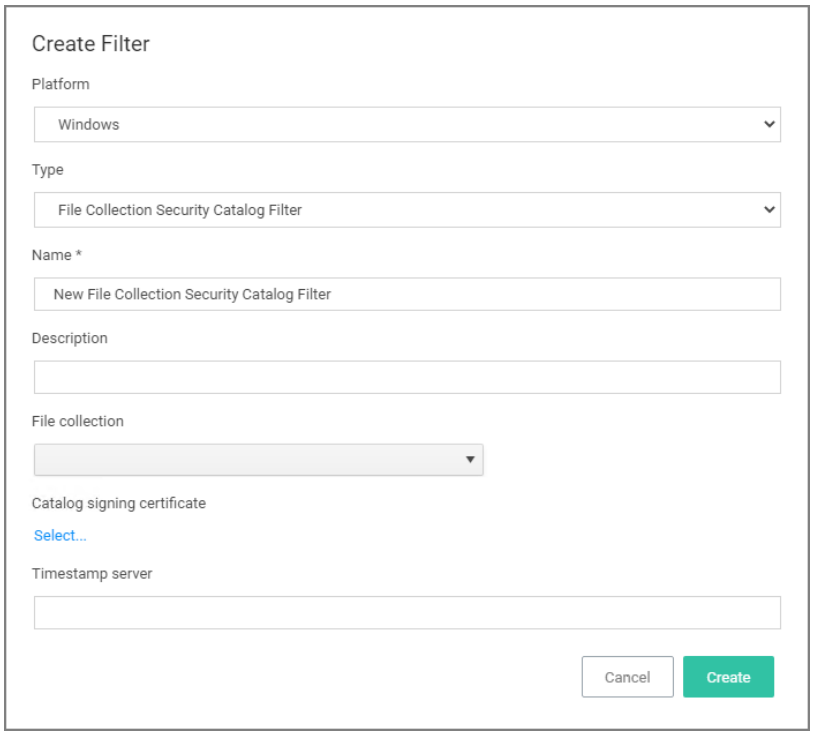
- As Invoker
- Highest Available
- Require Administrator

Remember to **Save Changes** after any customization.

File Collection Security Catalog Filter

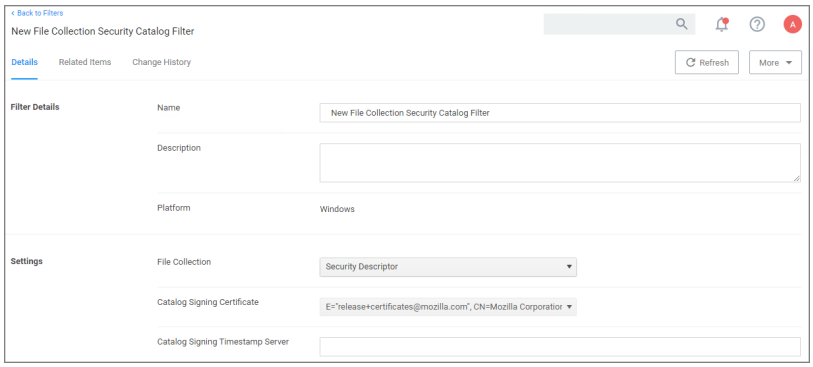
This is a special collection of files allow or deny list. This filter type is similar to other Inventory Filters, particularly our Security Catalog Filter. *No out-of-box filters exist in Privilege Manager for this type*.

You can use these filters to target executables found in security catalogs. The built-in filter targets the Signed Security Catalog (\Windows\System32\catroot) and is typically used to automatically allow list applications from Microsoft.



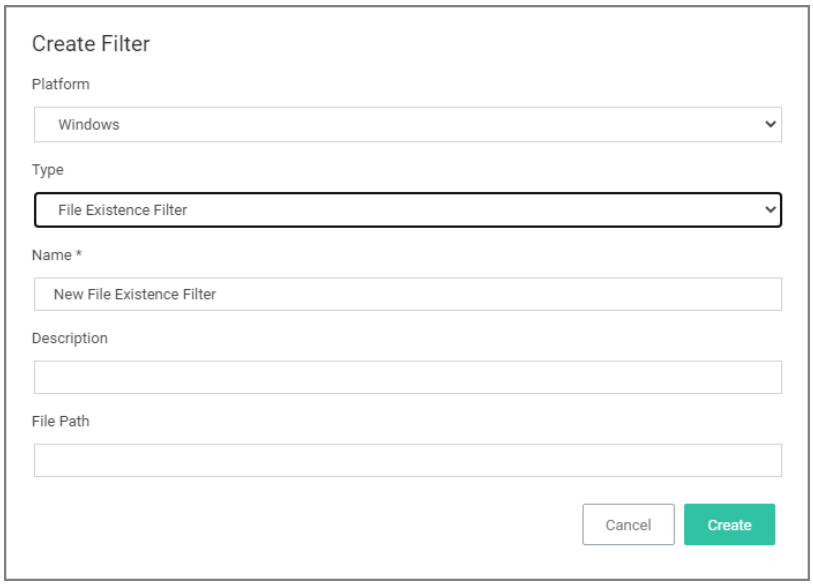
Parameters

- File collection, this is the specific catalog you want to use.
- Catalog signing certificate, select the specific certificate from a list.
- Timestamp server, specifies a particular version to be used.



File Existence Filter

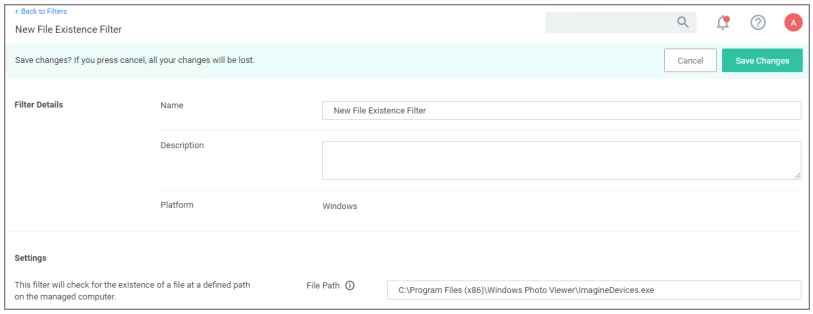
This type of filter identifies whether a file exists. *No out-of-box filters exist in Privilege Manager for this type*.



This filter is available for both Windows and macOS systems.

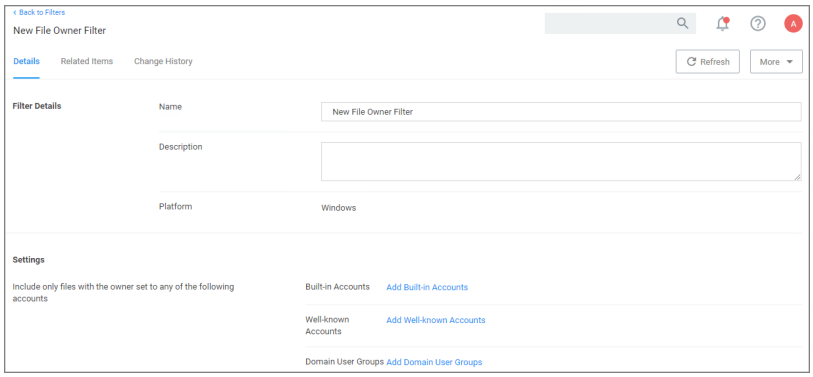
Parameters

Path, this must be an exact file path. Windows Environment Variables are supported though, %ProgramFiles% for example.



File Owner Filter

This filter identifies files based on ownership.

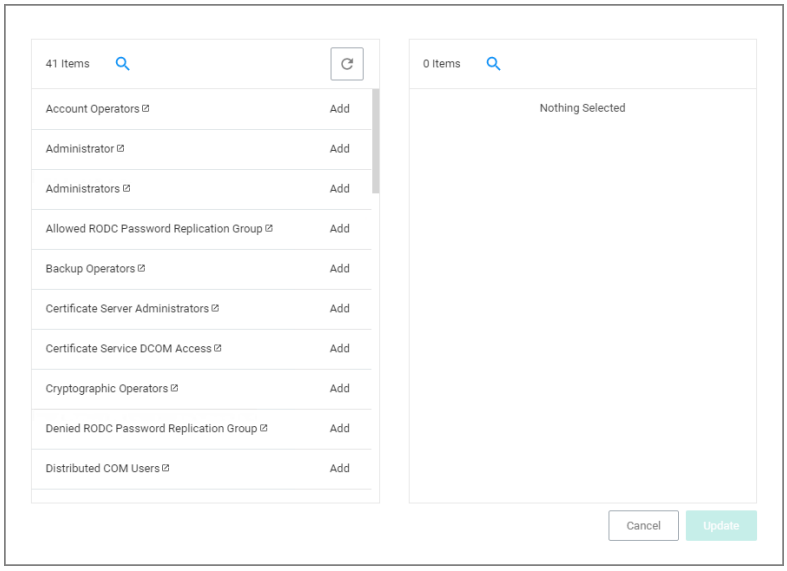


This filter is available for both Windows and macOS systems.

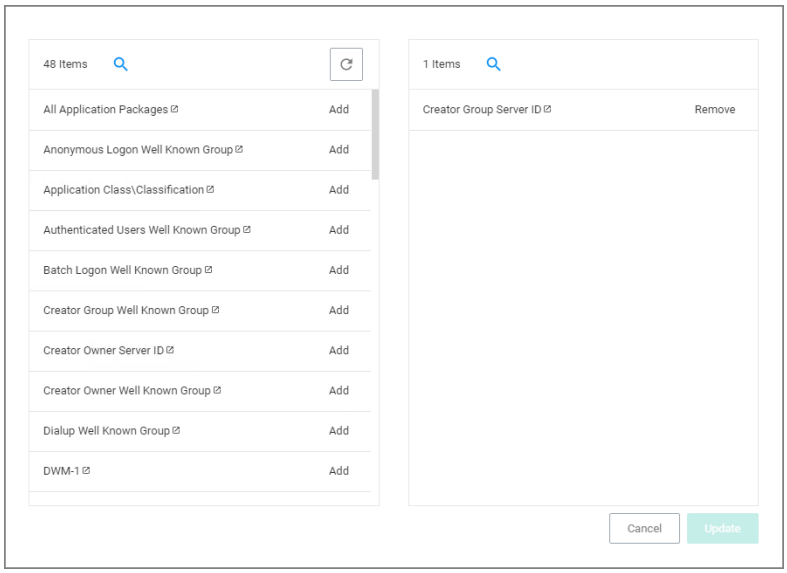
Parameters

Under settings you specify to include only those files with an owner having certain accounts or being part of certain domain user groups.

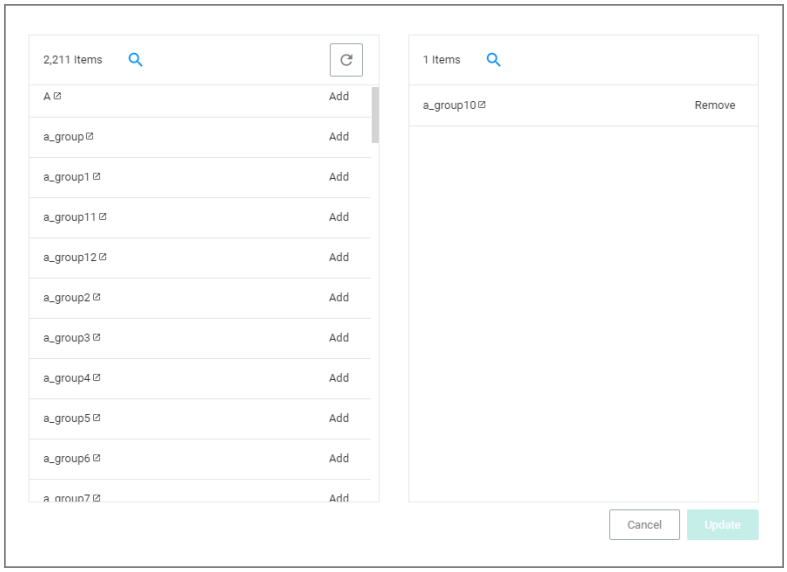
- Build-in Accounts



- Well-known Accounts



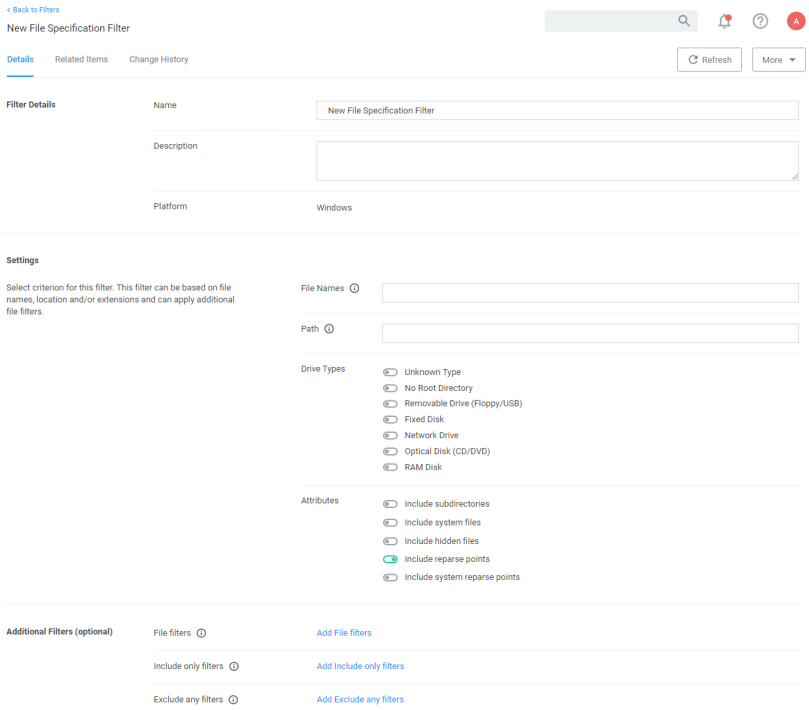
- Domain User Groups



Remember to click **Update** and **Save Changes** following any customization.

File Specification Filter

This filter identifies files based on their file name, extension, path, or location on a computer.



This filter is available for both Windows and macOS systems. Use this filter for macOS endpoints only to target known scripts or command-line tools; otherwise use the Default File Specification (macOS) filter.

Parameters

- File Names
- Path
- Drive Types
- Attributes, include reparse points is the only default enabled attributes

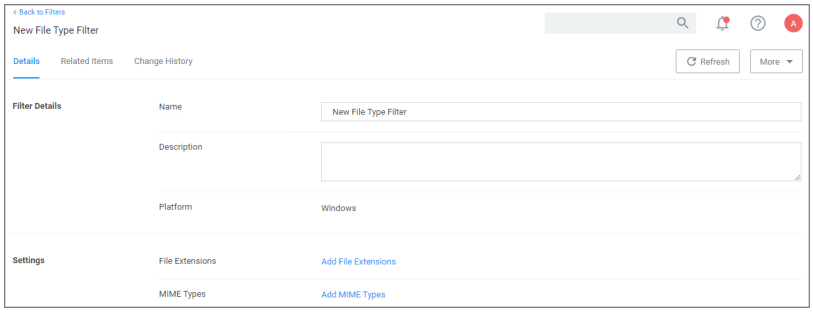
Additional Filters

Additional Filters can be added optionally.

- File filters, at least one of the filters added here must match.
- Include only filters, all of the filters added here have to match.
- Exclude any filters, any matching filters added here will be excluded.

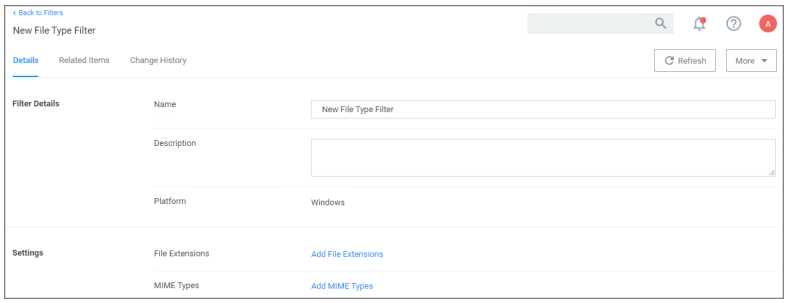
File Type Filter

This filter identifies files based on what type of file it is. *No out-of-box filters exist in Privilege Manager for this type*.

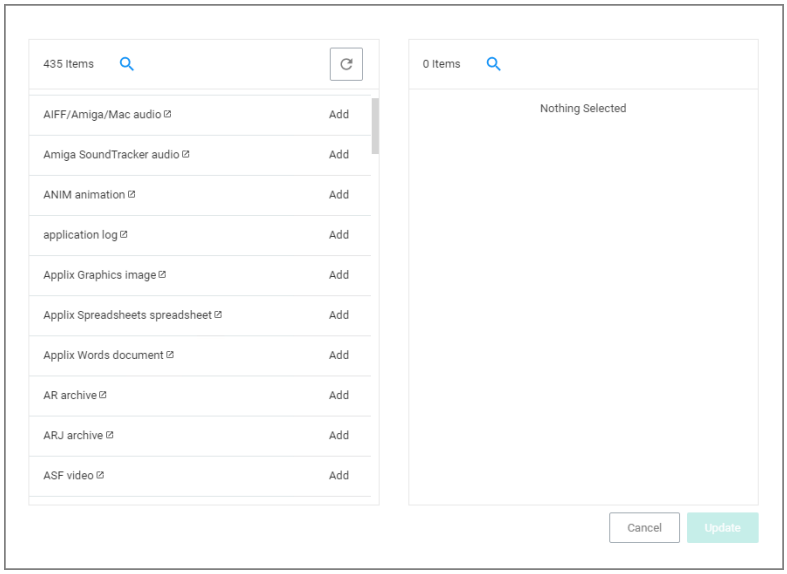


Parameters

- File Extensions



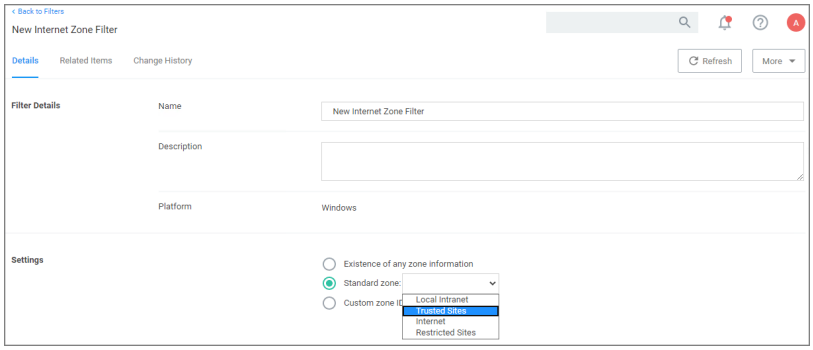
- MIME Types



Add the parameters, click **Update** and **Save Changes**.

Internet Zone Filter

This filter identifies what internet zone a computer is connected to on your network, such as Trusted Sites and Local Intranet. *No out-of-box filters exist in Privilege Manager for this type*.

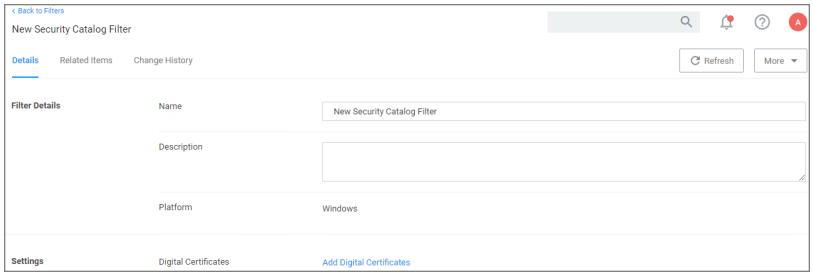


Parameters

- Existence of any zone information
- Standard zone:
  - Local Intranet
  - Trusted Sites
  - Internet
  - Restricted Sites
- Custom Zone IDs

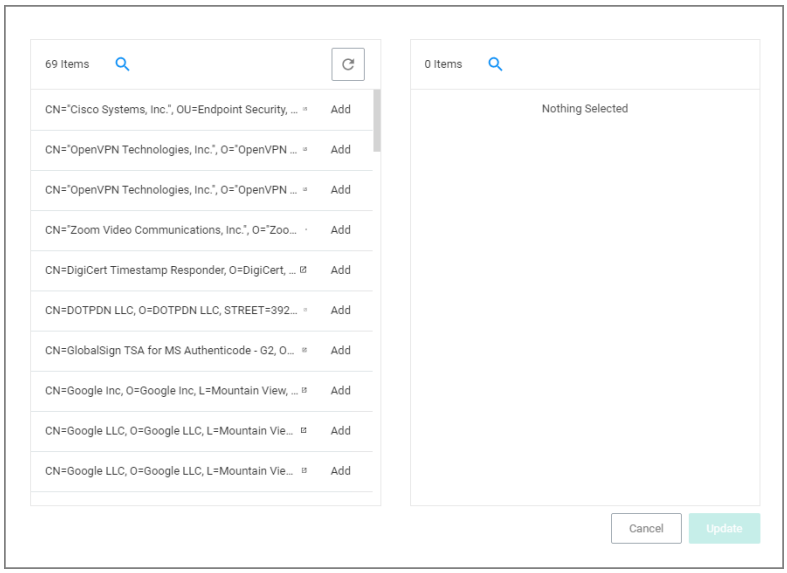
Security Catalog Filter

This is a special collection of files to allow or deny list. For example, the Microsoft Security Catalog is often allow listed as a trusted catalog.



Parameters

- Digital Certificates

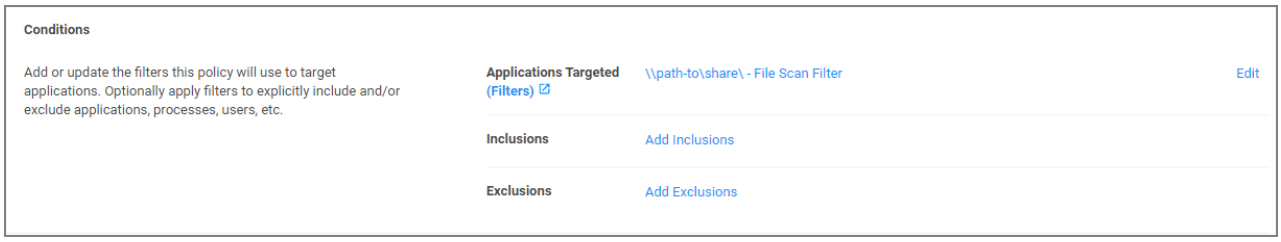


Unable to Access Cortana and Search for Windows 10

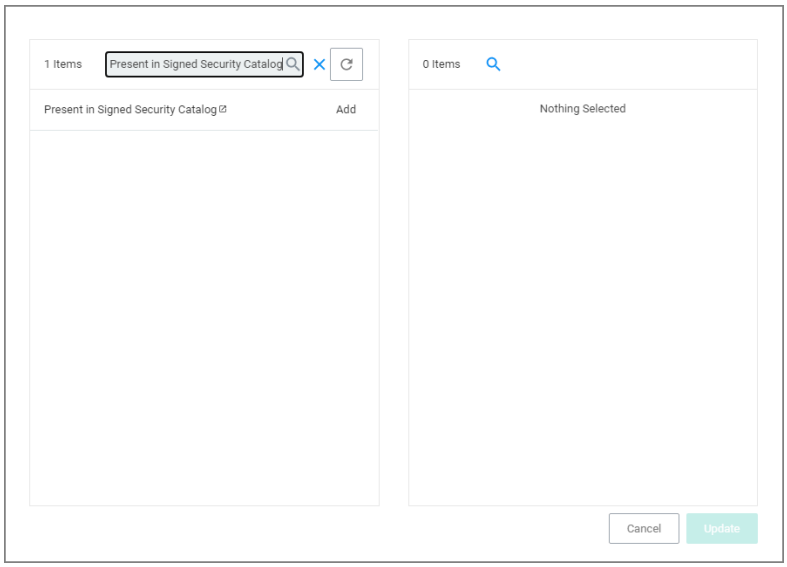
This issue might be due to the **Present in Signed Security Catalog** not being added to the **Exclusion Filters** section in a policy.

How to Resolve

1. Launch **$1Privilege Manager$2** and navigate to your **Application Policies**.
2. Click on a previously created policy.
3. Under **Conditions**, next to Exclusions select **Add Exclusion Filter**.



4. Search for **Present in Signed Security Catalog**.



5. Click **Add** next to the **Present in Signed Security** filter.
6. Click **Update**.
7. Click **Save Changes** on the policy page.

   Note: Once the agents check back into the web console which by default occurs every 30 minutes, the machines will get the new policy changes. However if you would like to test the policy update on a specific machine, please continue.

8. Go to the Machine(s) where you want to update the policy and open the Agent Utility.

   e.g., `C:\Program Files\Thycotic\Agents\Agent`

9. Click **Update**.

Inventory Filters

These depend on file inventory data, meaning they generally apply to already discovered applications or files pulled in by Privilege Manager tasks. For example, after running an inventory task on a specific computer or group of computers, Privilege Manager can use the list of files inventoried and target those files.

Note: No out-of-box filters exist in Privilege Manager for this type of filter category. Most filters of this type are associated with a data source during their creation. That data source is not to be changed. The exception is the Security Catalog File Filter where the data source needs to be added after the filter has been created.

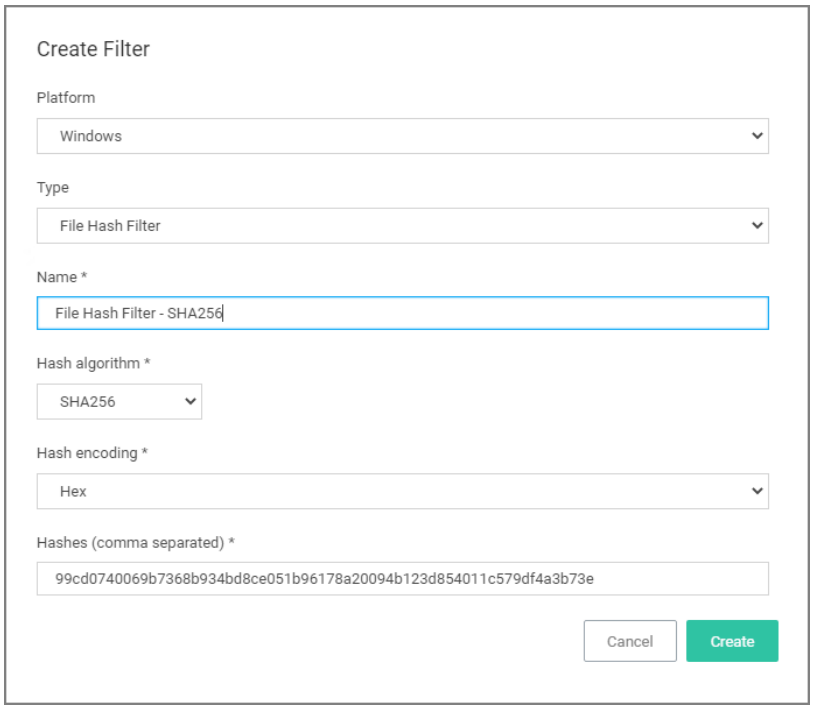
The following Inventory Filter type filter topics are available:

- File Hash Filter
- File Scan Results Filter - Computer
- File Scan Results Filter - Policy
- MSI File Contents Filter
- MSI Package Contents Filter
- Package Contents Filter
- Security Catalog Contents Filter
- Virtual Disk File Contents Filter
- Virtual Disk Package Contents Filter

File Hash Filter

This type of filter identifies files inventoried based on Hash Algorithms. *No out-of-box filters exist in Privilege Manager for this type*.

When creating this filter, the target hashes need to be entered as a comma-separated list:



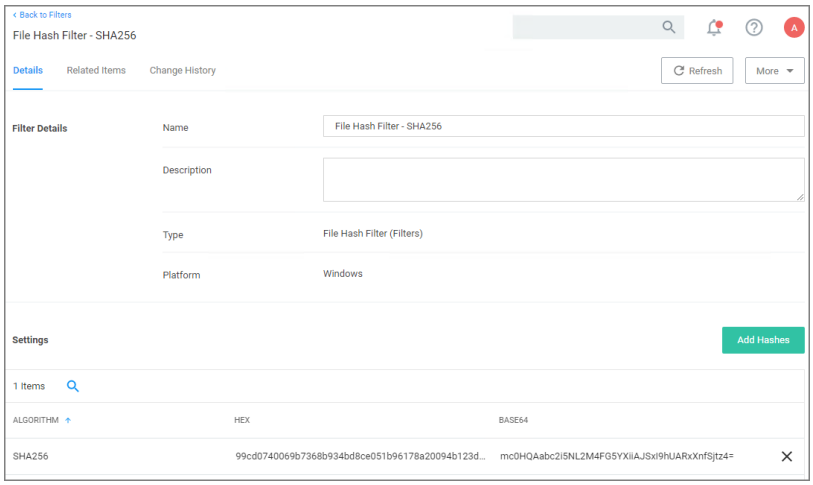
This filter is available for macOS, Unix/Linux, and Windows systems.

Required Parameters on Filter Creation

- **Hash algorithm** drop-down, only one can be specified per filter:
  - MD5
  - SHA1 (only for backwards compatibility - should not be used anymore!)
  - Authenticode
  - SHA256
  - Authenticode 2
- **Hash encoding** drop-down:
  - Hex
  - Base64
- **Hashes (comma separated)** text field.

Example of SHA256 Filter

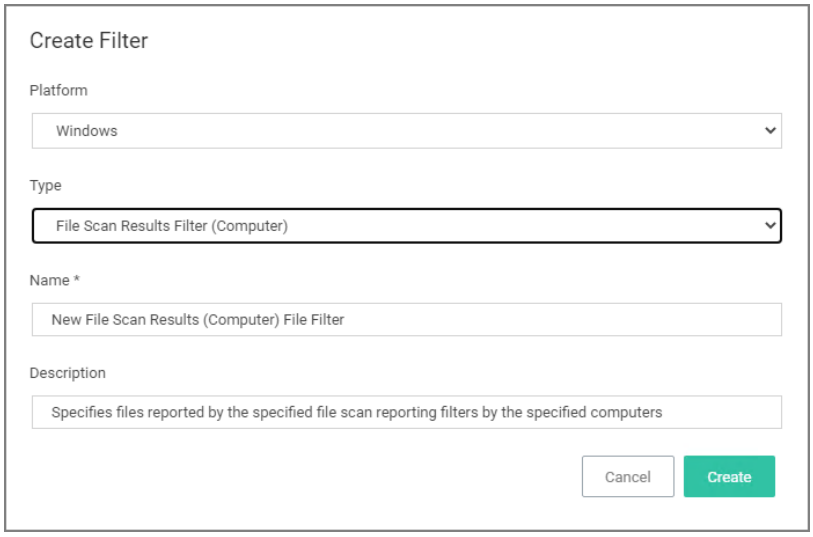
Once the filter is created, the following settings can be viewed and/or edited:



Algorithm, in hex and base64 format. Algorithms and hashes can be added via the **Add Hashes** button.

File Scan Results Filter (Computer)

This type of filter identifies file inventory based on another computer's file scan results. This allows for one computer that has been setup properly to be used as a source for this filter. *No out-of-box filters exist in Privilege Manager for this type*.

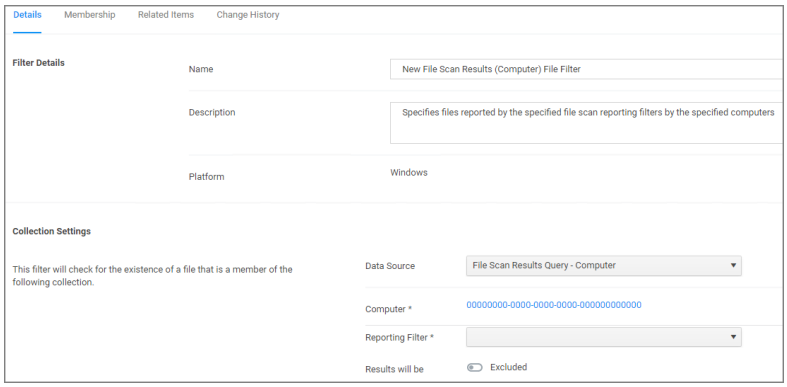


This filter is available for both Windows and macOS systems.

Parameters

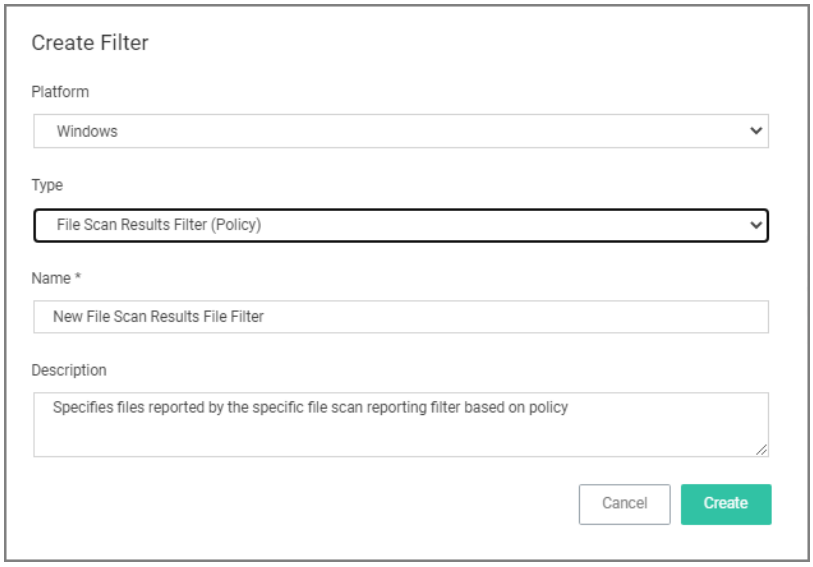
Once the filter is created the following settings can be viewed and/or edited:

- Data Source, this **should not be edited**. The information here is specific to the task of the File Scan Results Filter for computers.
- Computer, this is the actual computer resource that has to be selected for the scan.
- Reporting Filter
- Results will be either excluded (default) or included.



File Scan Results Filter (Policy)

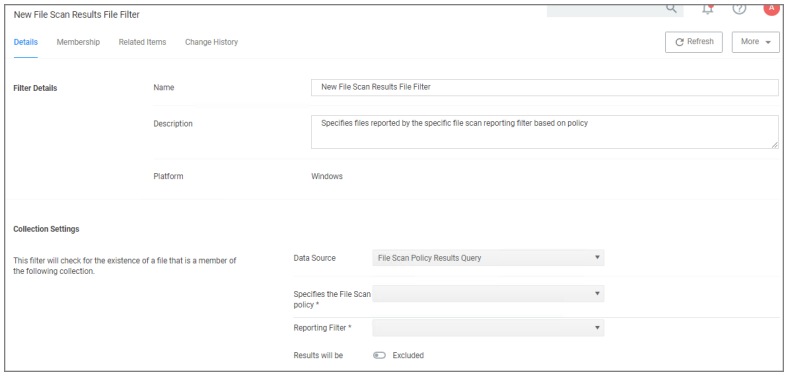
This type of filter identifies file inventory based on Privilege Manager Policies. *No out-of-box filters exist in Privilege Manager for this type*.



Parameters

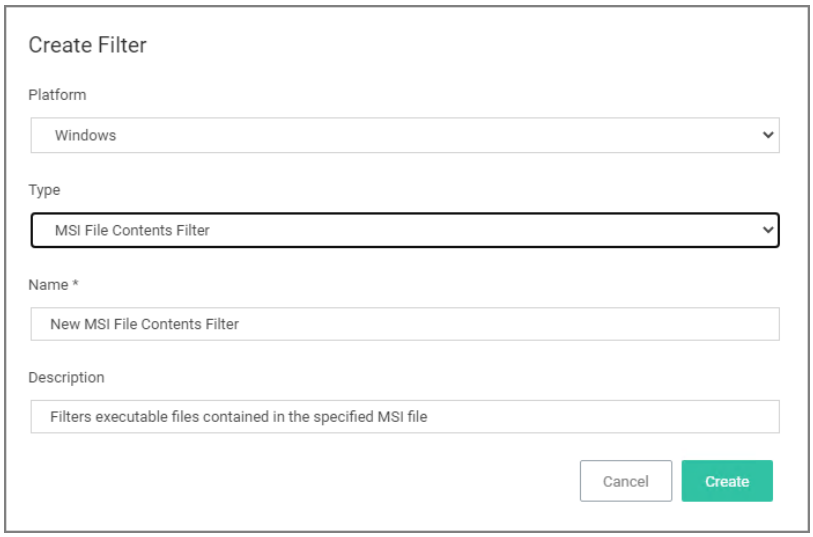
Once the filter is created the following settings can be viewed and/or edited:

- Data Source, this **should not be edited**, it is the File Scan Policy Results Query.
- Specifies the File Scan Policy, this is the actual Policy resource that has to be selected for the scan.
- Reporting Filter
- Results will be either excluded (default) or included.



MSI File Contents Filter

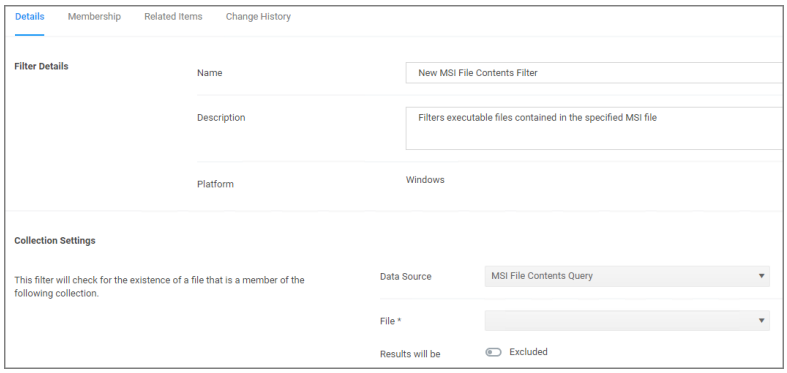
This type of filter identifies file inventory based on .MSI file contents, i.e. specific Windows package installers. *No out-of-box filters exist in Privilege Manager for this type*.



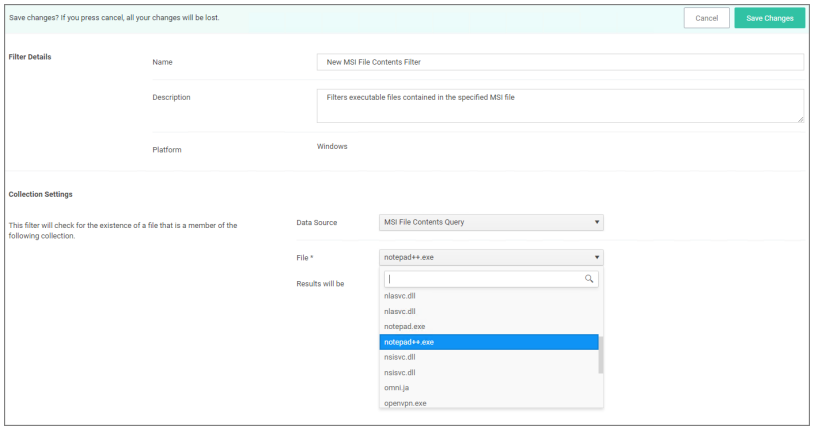
Parameters

Once the filter is created the following settings can be viewed and/or edited:

- Data Source, (**do not edit**) this is the MSI File Contents Query.
- File:
  - Parameters (these are required)
    - Win32 Executable
    - Product Name
  - Select Resource, this is the actual MSI file resource that has to be selected for the scan.
- Results will be either excluded (default) or included.

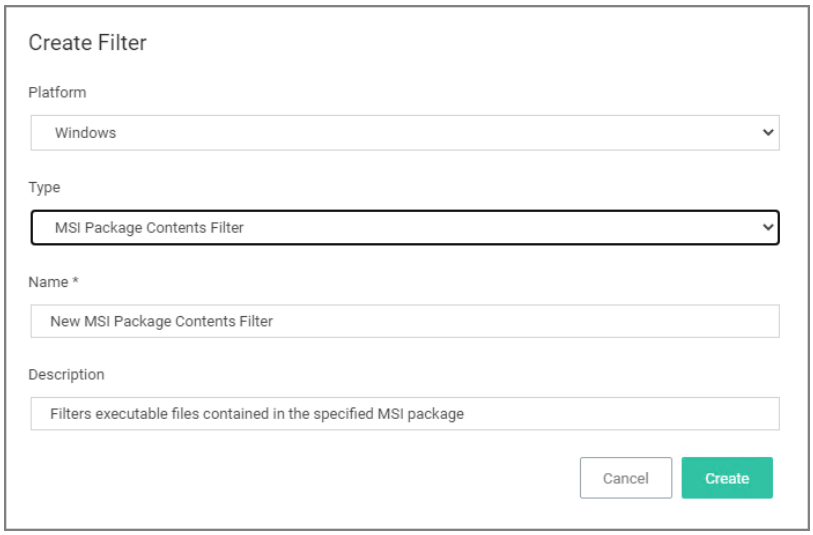


Viewing, Editing, and Saving the Parameters



MSI Package Contents Filter

This type of filter identifies file inventory based on MSI package contents. *No out-of-box filters exist in Privilege Manager for this type*.



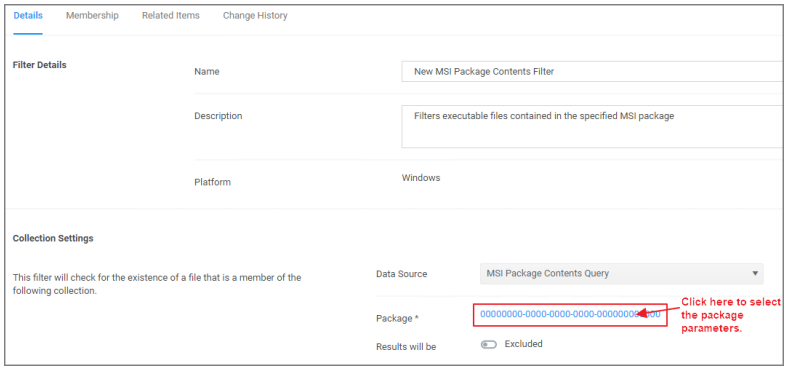
Parameters

Once the filter is created the following settings can be viewed and/or edited:

- Data Source, (**do not edit**) this is the MSI Package Contents Query.
- Package:

- Parameters:
  - Scope by Organizational Group
  - Search text
  - Maximum rows returned, this is a required parameter and the default is 10000.
- Select Resource, this is the actual MSI package resource that has to be selected for the query.

- Results will be either excluded (default) or included.

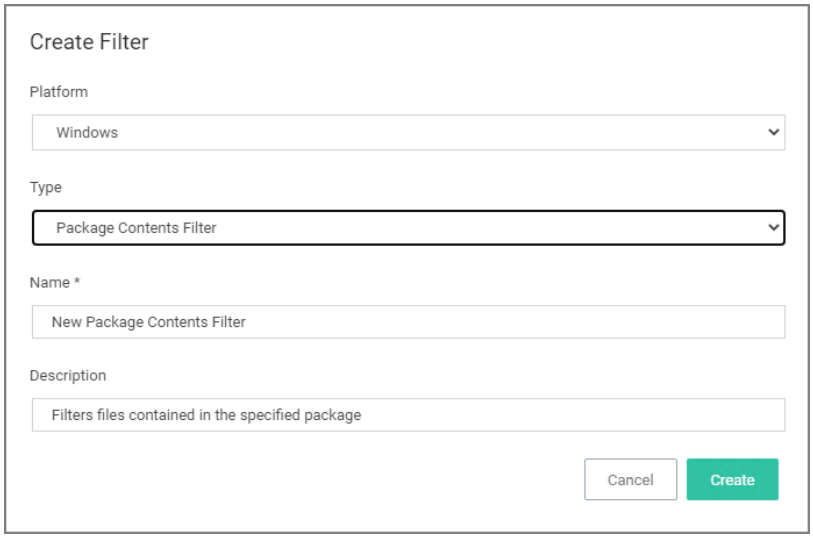


Viewing and Editing the Package Parameters

Viewing and Adding the Resource(s)

Package Contents Filter

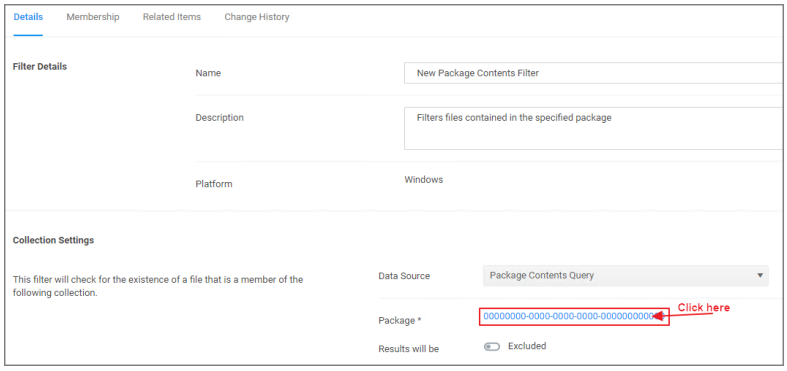
This type of filter identifies file inventory based on package contents. *No out-of-box filters exist in Privilege Manager for this type*.



Parameters

Once the filter is created the following settings can be viewed and/or edited:

- Data Source, (**do not edit**) this is the Package Contents Query.
- Package:
  - Parameters:
    - Scope by Organizational Group
    - Search text
    - Maximum rows returned, this is a required parameter and the default is 10000.
  - Select Resource, this is the actual package resource that has to be selected for the query.
- Results will be either excluded (default) or included.

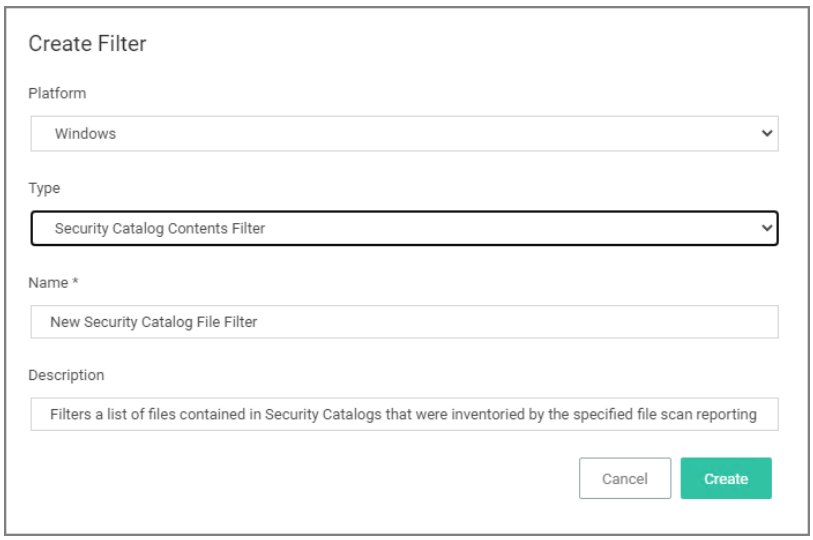


Viewing and Editing the Package Parameters

Adding the Resource(s)

Security Catalog Contents Filter

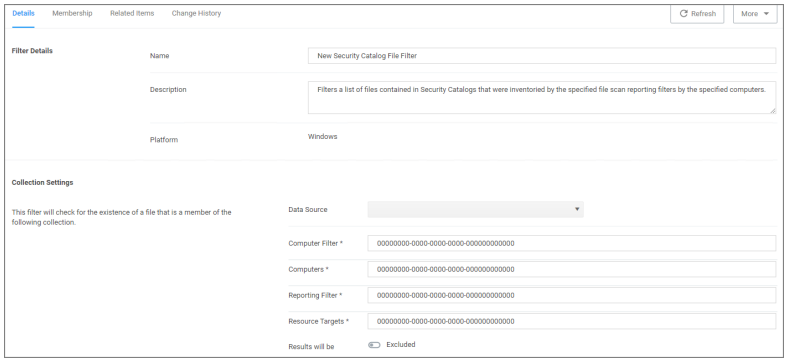
This is a special collection of files to allow or deny list. This filter type is similar to other Inventory Filters, particularly our Security Catalog Filter. *No out-of-box filters exist in Privilege Manager for this type.*



Parameters

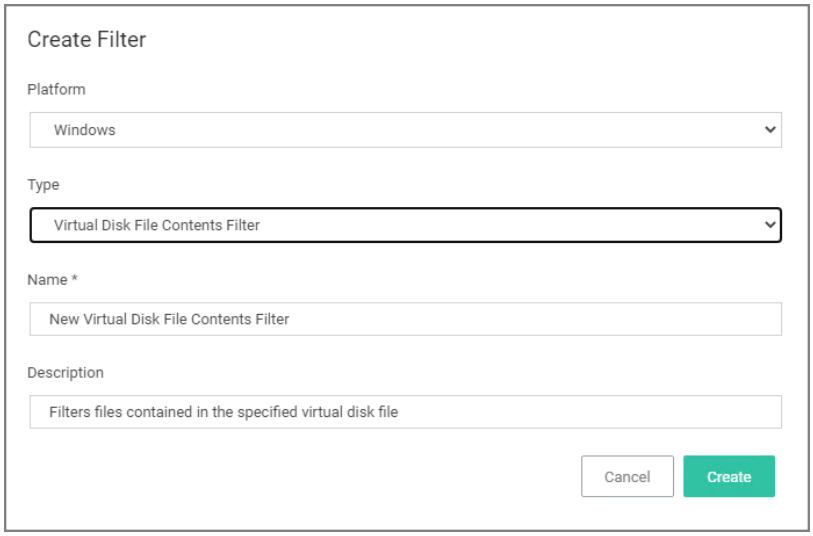
Once the filter is created the following settings can be viewed and/or edited:

- Data Source
- Computer Filter
- Computers
- Reporting Filter
- Resource Targets
- Results will be either excluded (default) or included.



Virtual Disk File Contents Filter

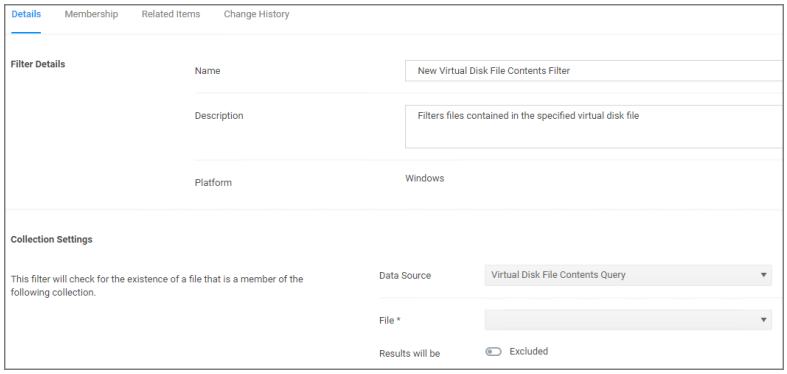
The Virtual Disk File Contents Filter filters files contained in the specified virtual disk file. *No out-of-box filters exist in Privilege Manager for this type*.



Parameters

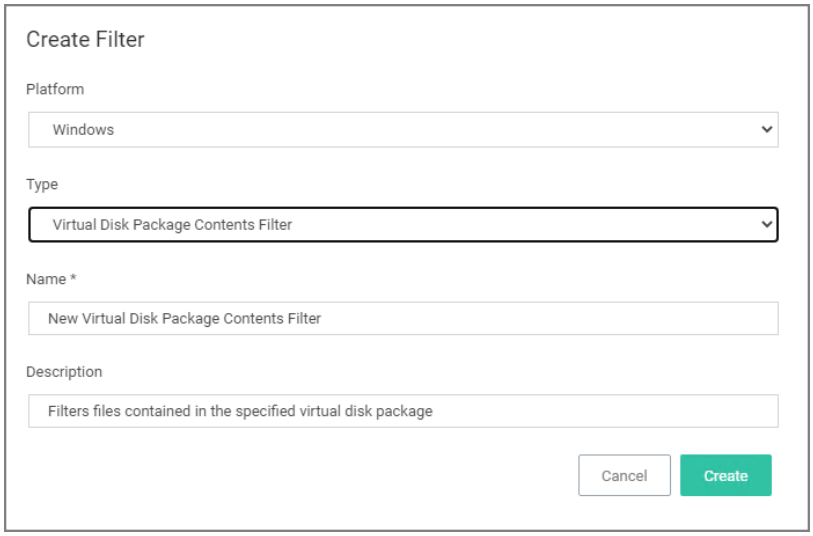
Once the filter is created the following settings can be viewed and/or edited:

- Data Source, (**do not edit**) this is the Virtual Disk File Contents Query.
- File, this is the actual virtual disk file resource that has to be selected for the scan.
- Results will be either excluded (default) or included.



Virtual Disk Package Contents Filter

Filters files contained in the specified virtual disk package. *No out-of-box filters exist in Privilege Manager for this type*.

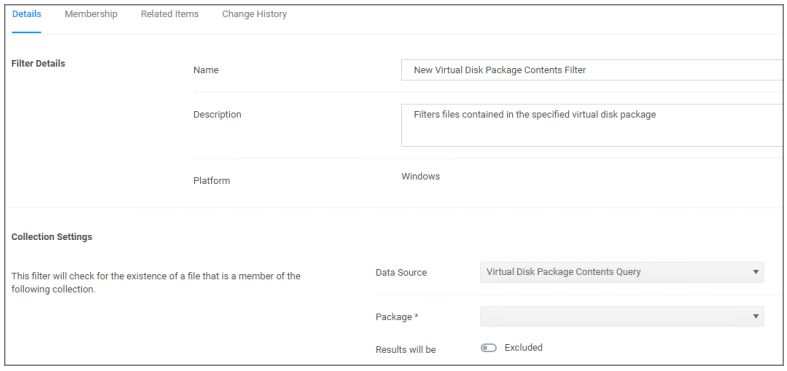


Parameters

Once the filter is created the following settings can be viewed and/or edited:

- Data Source, (do not edit) this is the Virtual Disk Package Contents Query.
- Package, select the actual package resource that is required for the query.

- Results will be either excluded (default) or included.



macOS Specific Filters

Most of the Application and File type filters apply to Windows as much as macOS platforms. There are some macOS specific filters that are covered in this section.

This is the default drop-down list when adding a new filter for macOS:

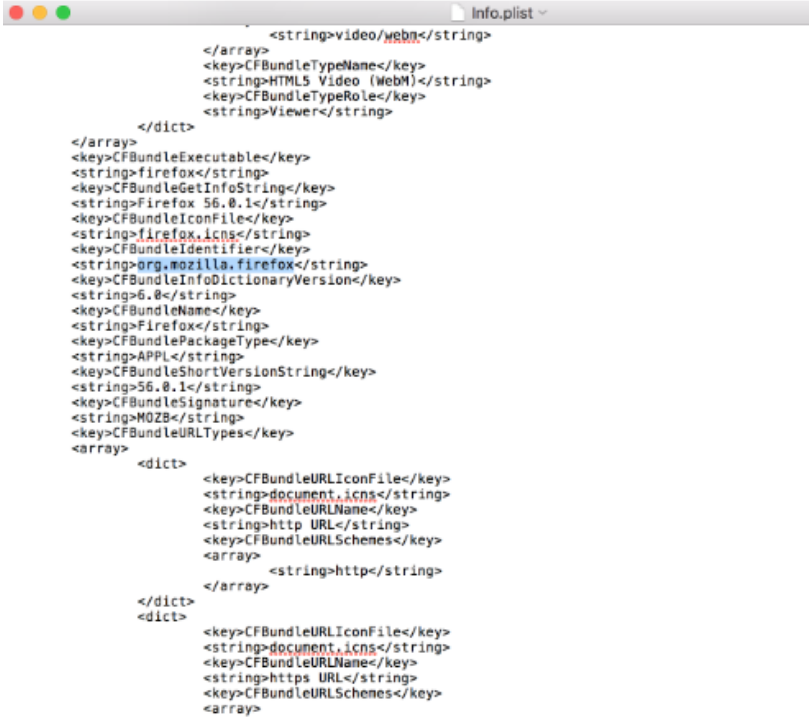
Creating macOS Filters Manually

In cases when Privilege Manager does not have enough information from the discovery process on a macOS endpoint, filters have to be created manually.

To manually find granular information required for targeting applications in Privilege Manager on a macOS endpoint,

1. Right-click the target application and select **Show Package Contents**.
2. Navigate to **Contents | Info.plist**, this gives you a coded list of items that you can match into the details page of your Filter.

For example, the highlighted section below can be entered into the **Bundled Identifier** line item when creating a Firefox filter.



List of macOS Filters

The following filters are available based on type from a quick select drop-down menu, after choosing macOS as the platform.

Application Filter Types

- Commandline Filter
- Download Source Filter
- Parent Process Filter
- Secondary File Filter
- Security Rating Filter
- Signed File Filter
- Time Of Day Filter
- User Context Filter
  - Leveraging the User Context Filter for NoMAD

File Filter Types

- Application Bundle Filter
- File Hash Filter
- File Existence Filter
- File Owner Filter
- File Scan Results Filter (Computer)
- File Specification Filter

List of Default Filters for Event Discovery

The following filters are the default filters used during inventory event discovery on macOS endpoints:

- Default File Specification (macOS)
  - Default Applications Folder (macOS)
  - System Applications Folder (macOS)
- Default App Bundles File Specification Filter
  - Default Application Bundles Filter (macOS)
  - System Application Bundles Filter (macOS)

Available Preference Pane Filters

- Date and Time Preference Pane filter
- Energy Saver Preference Pane filter
- Network Preference Pane filter

Application Bundle Filter

This type of filter identifies application bundles for macOS systems.

Prior to Privilege Manager v10.7.1, the value of the Bundle Name field required the inclusion of the .app extension (e.g. Console.app). The Bundle Name field should have an entry like **console.app** or **photos.app** to correctly apply the filter. If it is not present, the filter will fail to properly match. With Privilege Manager v10.7.1, the presence of the .app extension is properly calculated during policy processing.

Pre-10.7.1 Example

The bundle name should appear when creating the filter.

Parameters

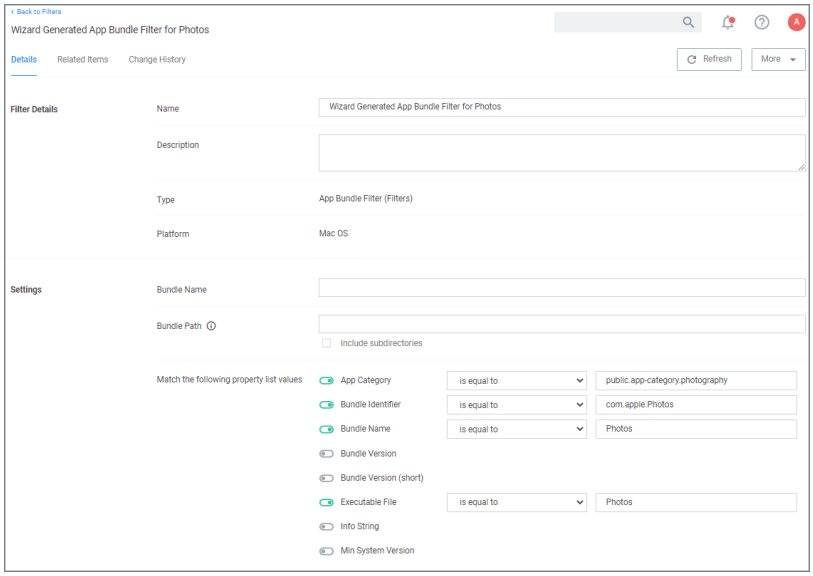
- Bundle Name
- Bundle Path
  - Include subdirectories

The following bundle properties can be used to identify an application bundle in an Application Bundle filter. These properties are found in the info.plist for the application on macOS systems.

- App Category
- Bundle Identifier
- Bundle Name
- Bundle Version
- Bundle Version (short)
- Executable File

- Info String
- Min System Version

Note: The **Bundle Name** field is separate from the Bundle Name in the property list. If you have the Bundle Name field populated and it doesn't match the binary being executed, the filter will fail to match and not process the property list values in the Info.plist file. If an app is discovered as a new loaded resource and assigned to a policy, a filter is created and pre-populated based on the information pulled from the info.plist file.



Info.plist Example for Photos

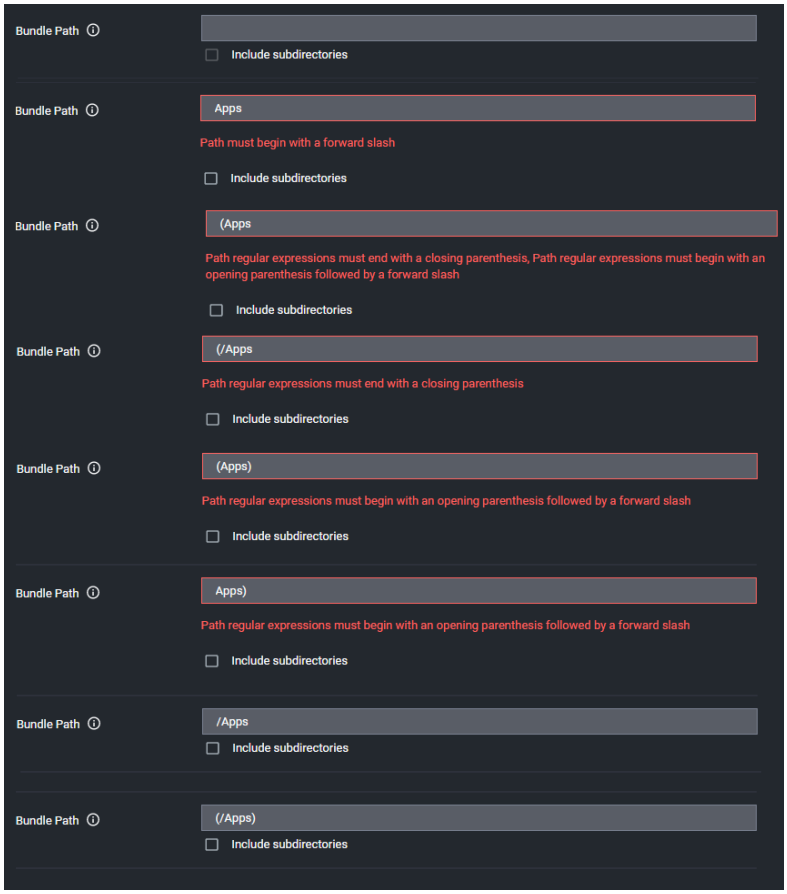
```
<key>CFBundleExecutable</key>
<string>Photos</string>
<key>CFBundleHelpBookFolder</key>
<string>Photos.help</string>
<key>CFBundleHelpBookName</key>
<string>com.apple.Photos.help</string>
<key>CFBundleIconFile</key>
<string>AppIcon</string>
<key>CFBundleIconName</key>
<key>CFBundleIdentifier</key>
<string>com.apple.Photos</string>
<key>CFBundleInfoDictionaryVersion</key>
<string>6.0</string>
```

Using RegEx in Bundle Path

The Bundle Path parameter supports RegEx. The RegEx must be surrounded by parenthesis and will be compared against the lowercase file path, for example "(/applications/.*)". When a RegEx is used for the Bundle Path, **Include subdirectories** is automatically disabled.

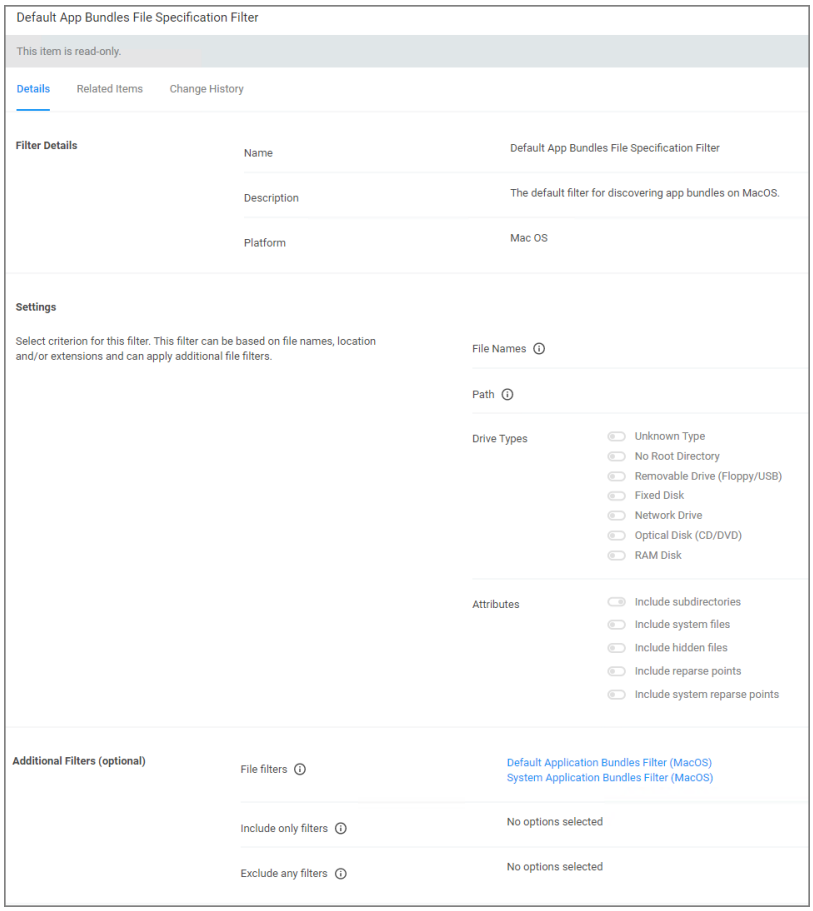
Validation error messages are provided when the

- Basic path is missing the leading `/`.
- RegEx path is missing the opening `(`.
- RegEx path is missing leading the `(/`.
- RegEx path is missing the closing `)`.



Default App Bundles File Specification Filter

This type of filter identifies application bundles for macOS systems. With this application bundles filter in place, macOS application bundles are inventoried regardless of their installation path in either /Applications or /System/Applications) on all versions of macOS.



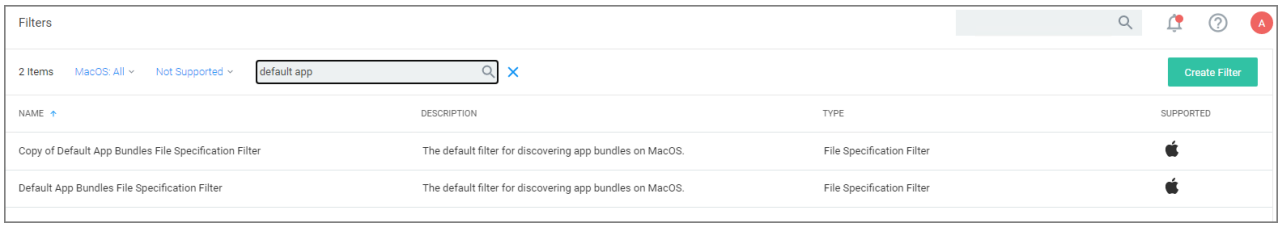
By default this is a read-only filter which uses the following Additional Filters:

- File filters:
  - Default Application Bundles Filter (macOS)
  - System Application Bundles Filter (macOS)

The option to include subdirectories is enabled by default.

Example

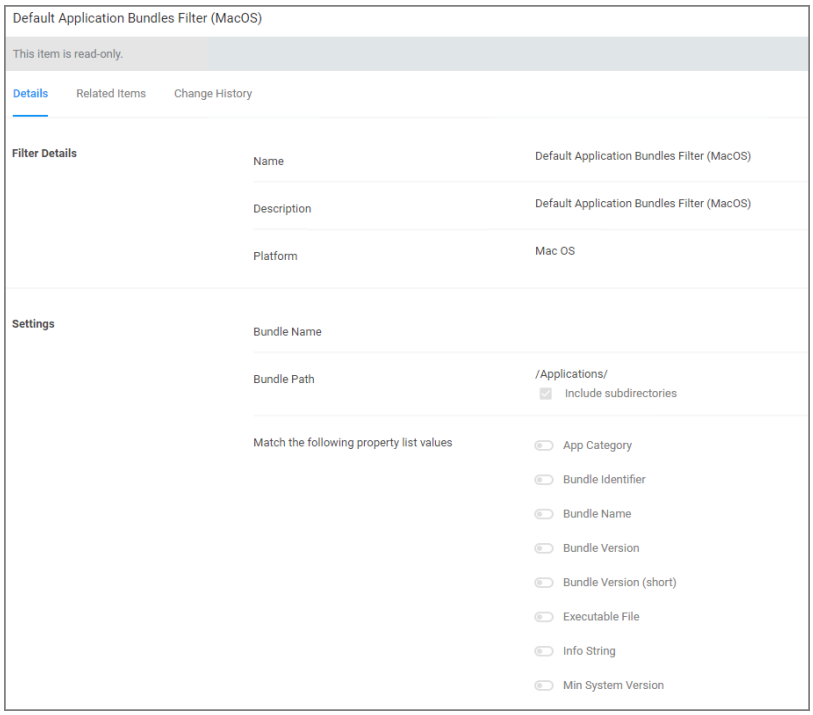
1. Navigate to **Admin | Filters**.
2. In the search field next to the supported/not supported OS drop-downs, search for *default app*.



3. Select the **Default App Bundles File Specification Filter** filter to view its details and/or create a copy to customize the filter.
4. Click **Duplicate**.
5. Set the needed parameters.
6. Click **Save Changes**.

Default Applications Bundle Filter (macOS)

The default filter for discovering application bundles in /Applications on macOS endpoints.

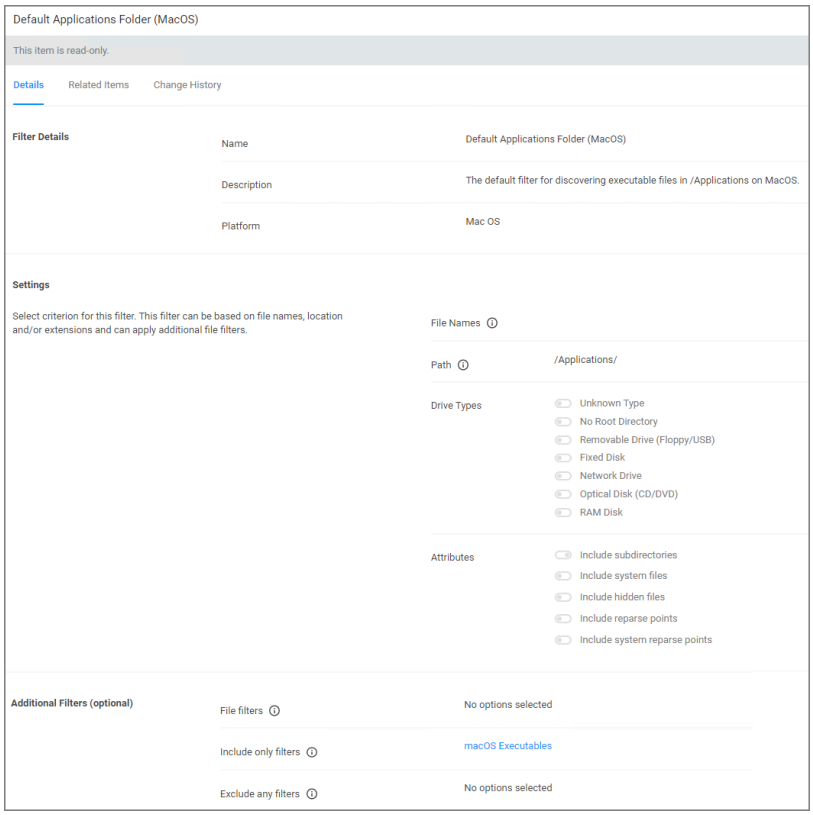


This filter is available for macOS systems.

The option to include subdirectories is enabled by default.

Default Applications Folder (macOS)

The default filter for discovering executable files in /Applications on macOS.



This filter is available for macOS systems.

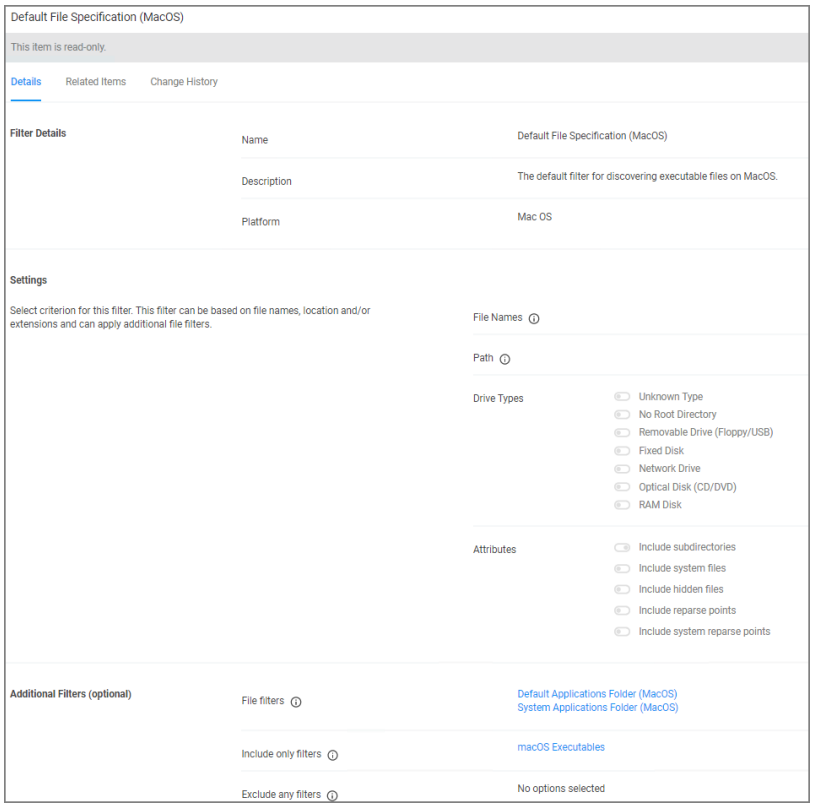
By default this is a read-only filter which uses the following Additional Filters:

- Include only filters:
  - macOS Executables

The option to include subdirectories is enabled by default.

Default File Specification (macOS)

This filter identifies files based on their file path or location on a computer.



This filter is available for macOS systems.

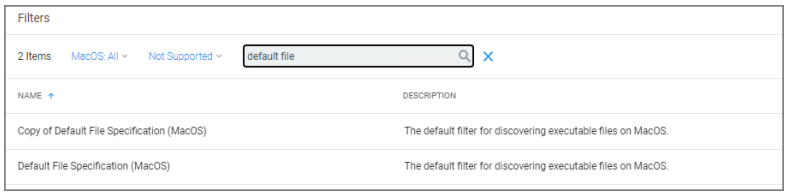
By default this is a read-only filter which uses the following Additional Filters:

- File filters:
  - System Applications Folder (macOS)
  - Default Applications Folder (macOS)
- Include only filters:
  - macOS Executables

The option to include subdirectories is enabled by default.

Example

1. Navigate to **Admin | Filters**.
2. In the search field next to the supported/not supported OS drop-downs, search for *default file*.

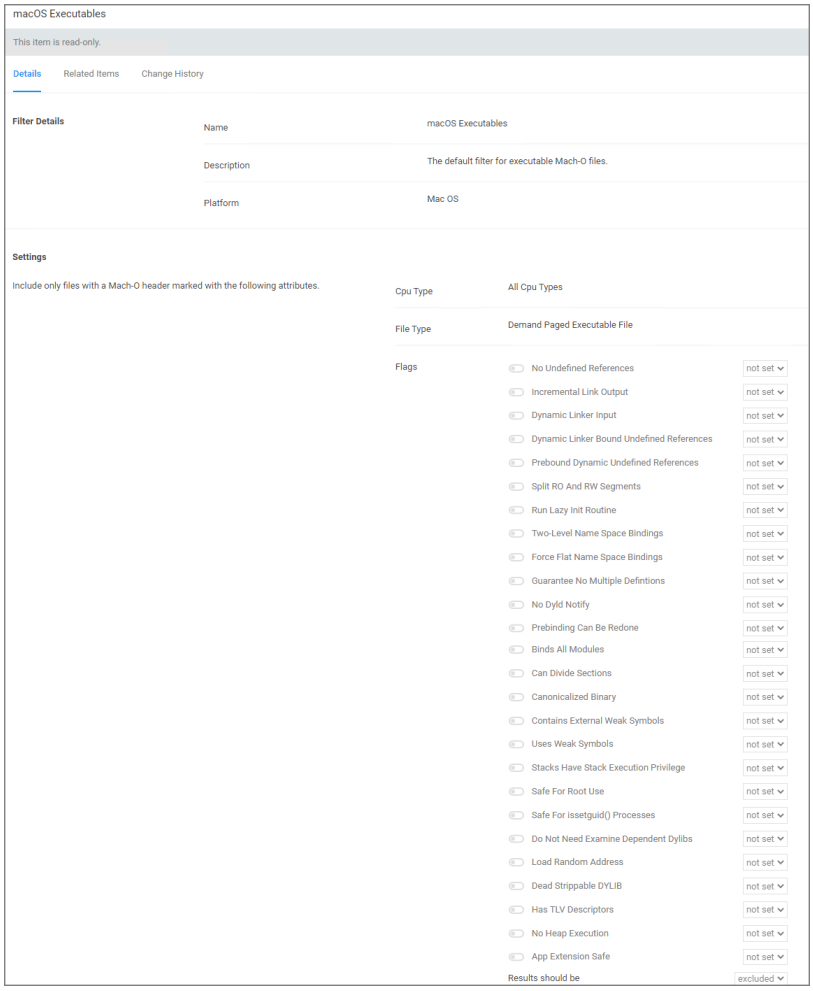


3. Select the **Default File Specification Filter (macOS)** filter to view its details and/or create a copy to customize the filter.
4. Click **Duplicate**.
5. Set the needed parameters.
6. Click **Save Changes**.

macOS Executables

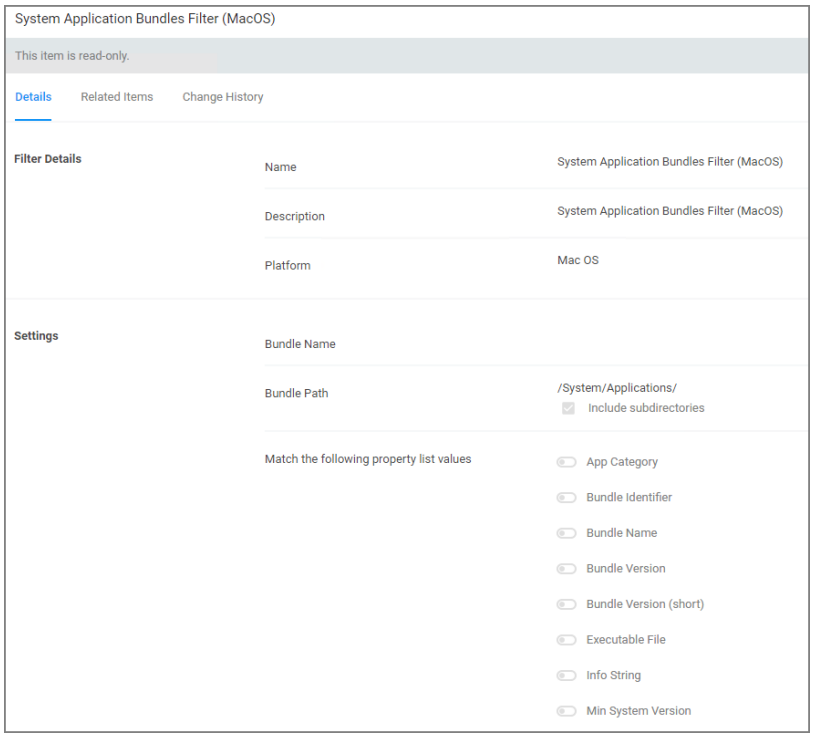
The default filter for executable Mach-O files. This filter is available for macOS systems.

Include only files with a Mach-O header marked with attributes set via the filter Settings:



System Application Bundles Filter (macOS)

The default filter for app bundles files in /System/Applications on macOS endpoints.

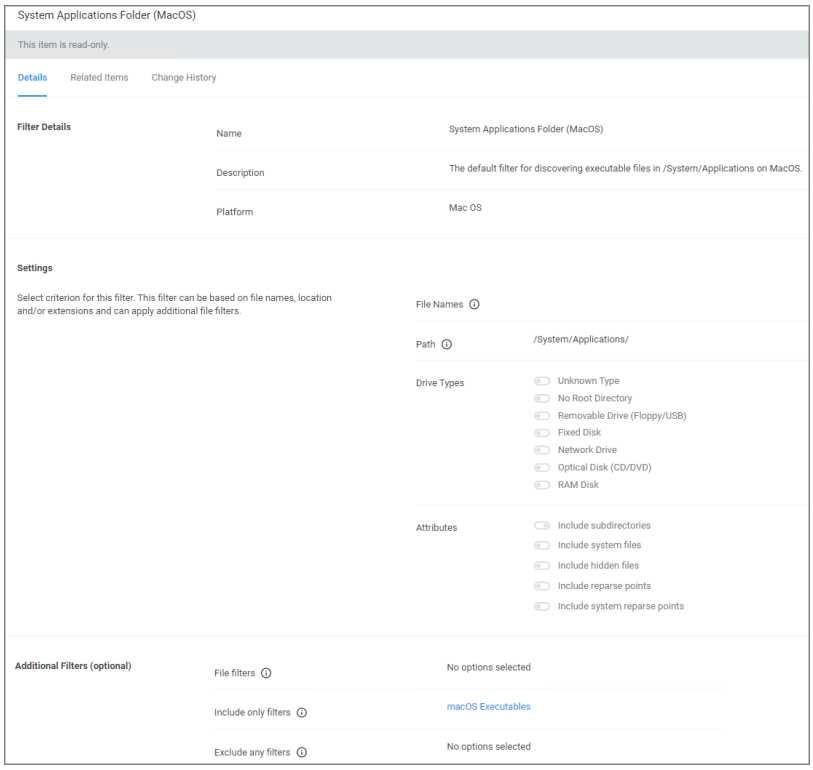


This filter is available for macOS systems.

The option to include subdirectories is enabled by default.

System Applications Folder (macOS)

The default filter for discovering executable files in /System/Applications on macOS endpoints.



This filter is available for macOS systems.

By default this is a read-only filter which uses the following Additional Filters:

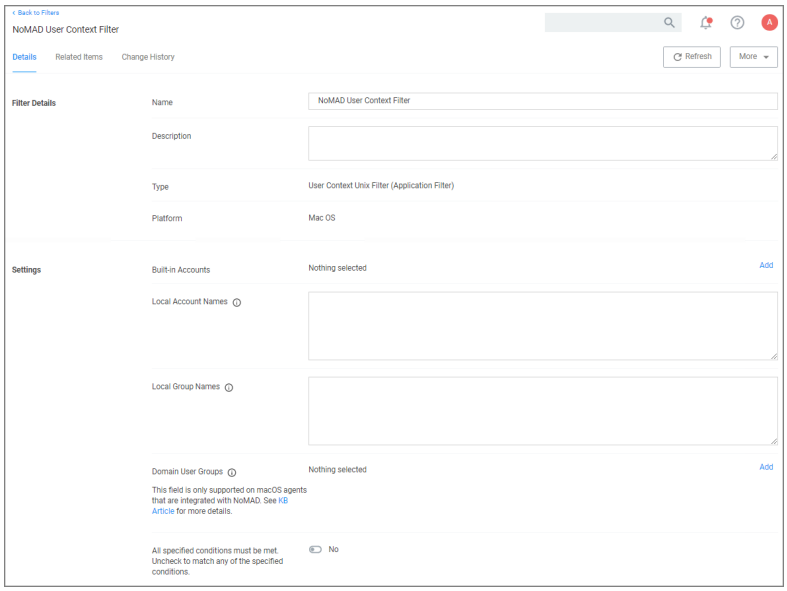
- Include only filters:
  - macOS Executables

The option to include subdirectories is enabled by default.

Leveraging the User Context Filter for NoMAD

Domain group memberships on macOS agents integrated with NoMAD can be targeted with a specific User Context filter.

1. Navigate to **Admin | Filters**.
2. Click **Create Filter**.
3. From the **Platform** drop-down, select **macOS**.
4. From the **Type** drop-down, select **User Context Filter**.
5. Name your filter to later search and easily find it for inclusion in policies.
6. Click **Create**.



7. Under **Settings | Domain User Groups**, click **Add**.
   a. On the **Select Resources** modal, enter a resource name for the search. Any group with the entered term in the name will be returned. If no name is entered all domain groups will be returned.
   b. Click **Search**.
   c. On the page with the list of returned resources, select the NoMAD integrated groups for this User Context Filter and click **Select**.
8. Click **Save Changes**.

You User Context Filter now contains the groups you associated with this filter, for example:

Note: If no groups are shown after the select resources search, you might have to run the Active Directory sync task to update available users and groups.

Refer to this video demonstration.

Preference Pane Filters

The following Preference Pane filters are supported for targeting in elevation type policies triggering justification and approval type interactive user dialogs:

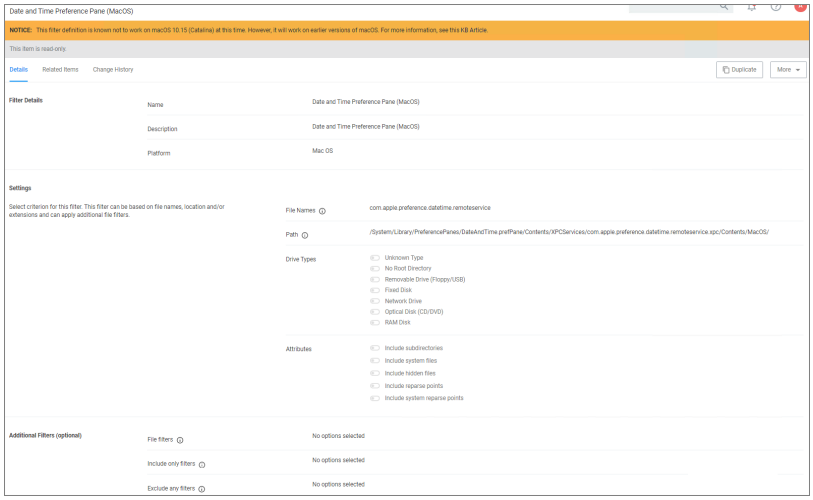
- Date and Time Preference Pane filter
- Energy Saver Preference Pane filter
- Network Preference Pane filter

For the following list of default Preference Pane filters, Delinea recommends to only target the preference pane in basic deny access policies:

- App Store Preference Pane
- Parental Controls Preference Pane
- Printers and Scanners Preference Pane
- Security and Privacy Preference Pane
- Sharing Preference Pane
- Time Machine Preference Pane
- Users and Groups Preference Pane

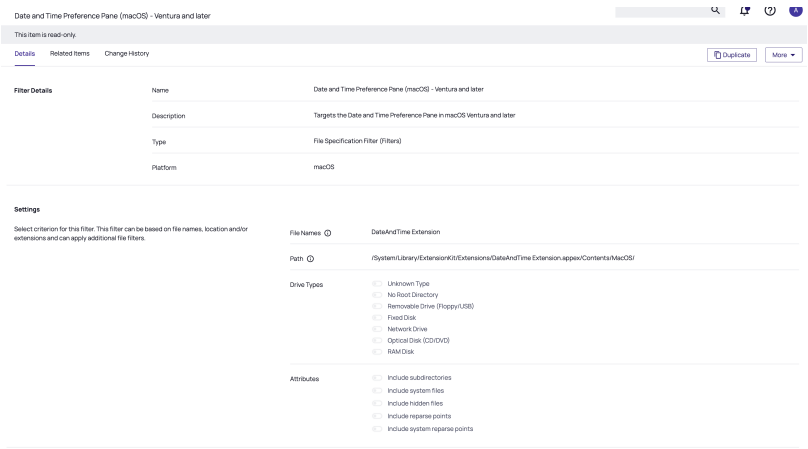
Date and Time Preference Pane Filter

The Date and Time Preference Pane filter is a read-only filter. If you need to customize the filter, create a copy and edit Settings and/or add Additional Filters.



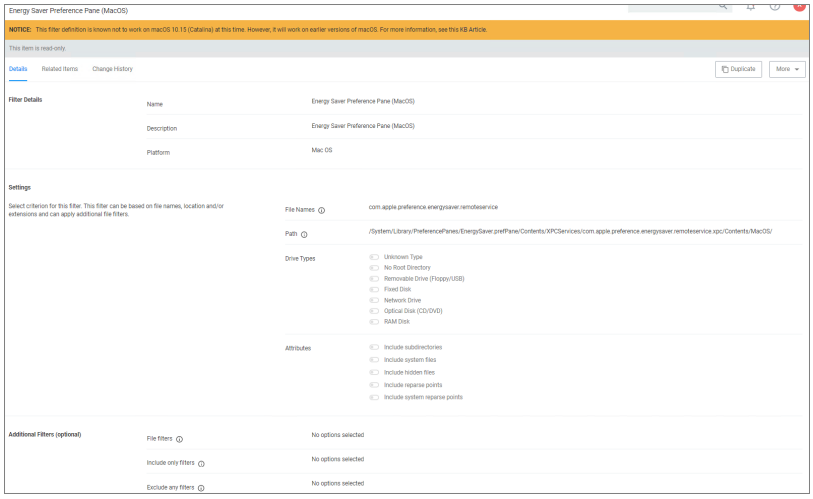
Once you create a duplicate, you can edit the default file names and path details. You can further specify to limit the targeting to specific drive type only based on selection, by default Delinea does not add any limitations here. Selecting Attributes allows to widen the default scope of the filter.

As shown here, the Date and Time Preference Pane filter is different for macOS Ventura and later.



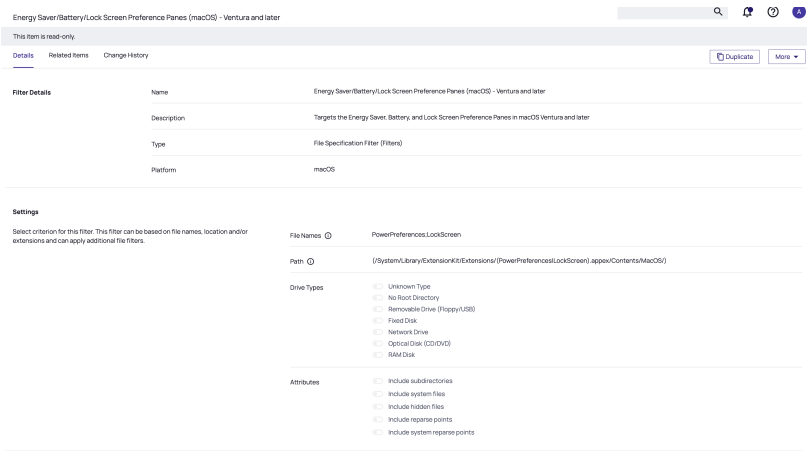
Energy Saver Preference Pane Filter

The Energy Saver Preference Pane Filter is a read-only filter. If you need to customize the filter, create a copy and edit Settings and/or add Additional Filters.



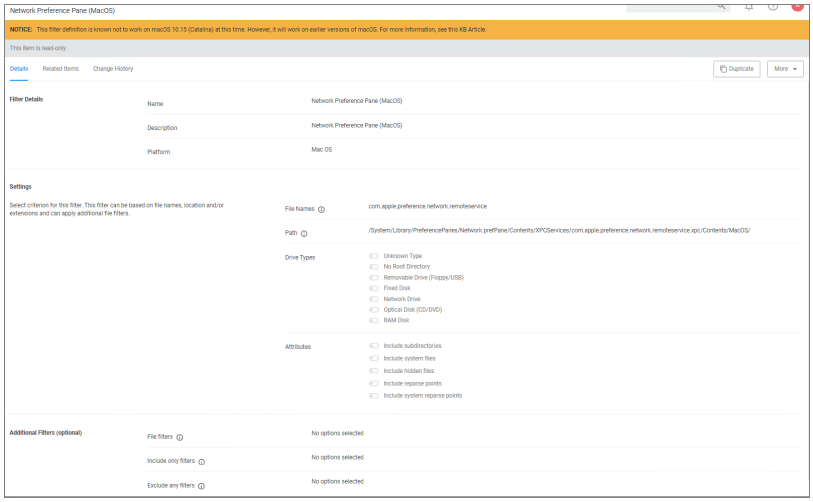
Once you create a duplicate, you can edit the default file names and path details. You can further specify to limit the targeting to specific drive type only based on selection, by default Delinea does not add any limitations here. Selecting Attributes allows to widen the default scope of the filter.

The Energy Saver Preference Pane filter is different for Ventura and later macOS versions. The Energy Saver, Battery, and Lock Screen panes use the same system extension in macOS Ventura and later; therefore, you need to target them all together. The Ventura and later macOS version filter for Energy Saver/Battery/Lock Screen Preference Panes is shown here.



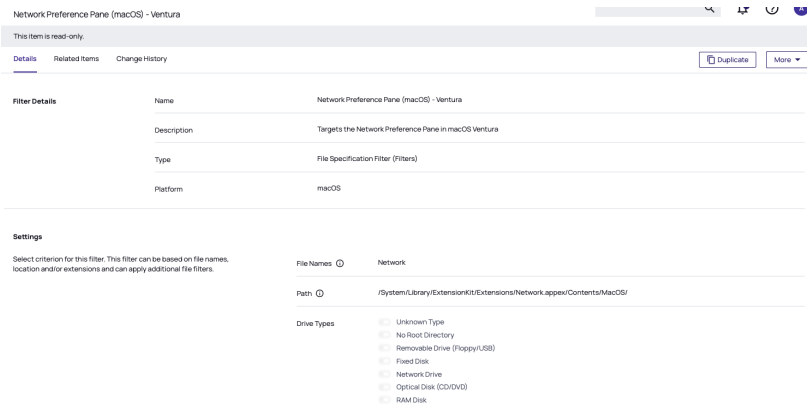
Network Preference Pane Filter

The Network Preference Pane Filter is a read-only filter. If you need to customize the filter, create a copy and edit Settings and/or add Additional Filters.



Once you create a duplicate, you can edit the default file names and path details. You can further specify to limit the targeting to specific drive type only based on selection, by default Delinea does not add any limitations here. Selecting Attributes allows to widen the default scope of the filter.

The Network Preference Pane filter, shown here, is different for macOS Ventura.



Unix/Linux Filters

Most of the Application and File type filters apply to all OS platforms. However, for Unix/Linux platforms, the filters are covered in this section.

Note: Privilege Manager for Linux/Unix and Windows for servers is End of Sale/Renewal only.

List of Unix/Linux Filters

The following filters are available based on type from a quick select drop-down menu, after choosing Unix/Linux as the platform.

- Advanced Commandline Filter
- File Hash Filter
- Time of Day Filter
- User Context Filter

Advanced Commandline Filter

This filter performs a Glob or RegEx match on the commandline submitted by Unix\Linux agent via sudo or pmsh. Commands can then be executed as they have been submitted or the filter has the ability to re-write the executed command via the Replacement field of the Command.

When adding commands, the Glob or RegEx is matched:

- Glob for simple filename matches such as *
- RegEx for advanced searches and matches of patterns in files such as ${pwd}

The command match is based on the command source, such as from the agent:

- The submitting user would only type a command such as sudo id, although the agent will submit the full path of the command such as `/usr/bin/id`.
- For security the command should be defined with the full executable path such as `/usr/bin/id` or `/bin/id`.

Arguments

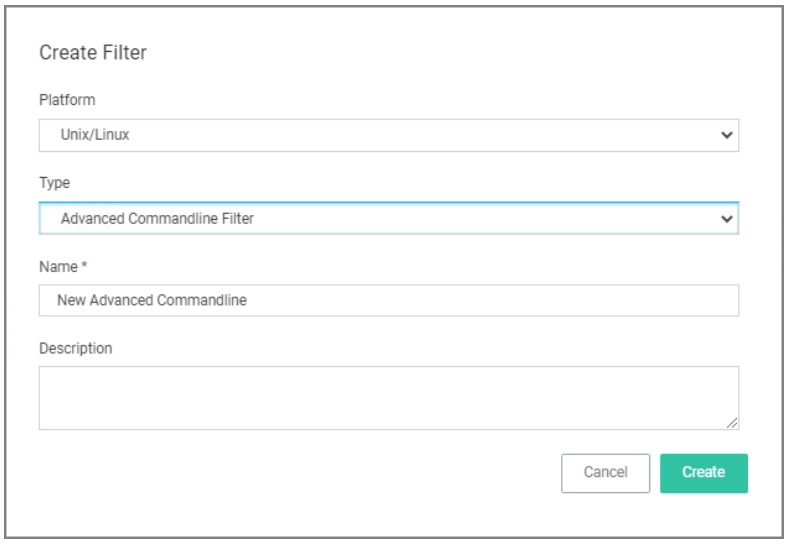
Allows more specific command submission matching from the agent such as `ls -l /root/*`.

Replacement

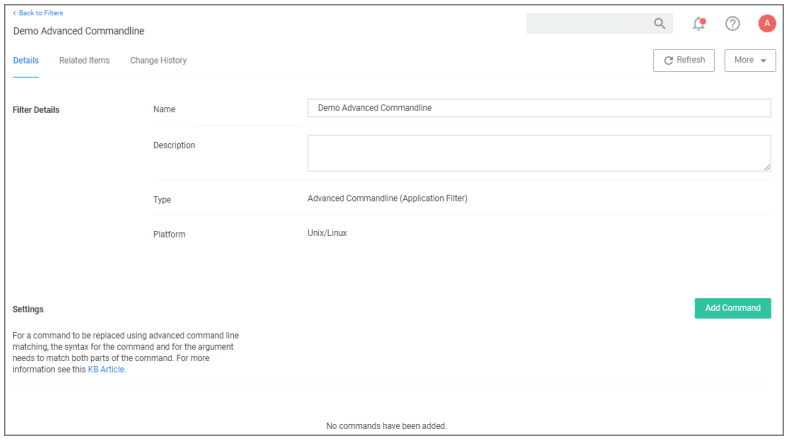
Rewrites the submitted command being executed on the Unix\Linux Agent

Creating a new Advanced Commandline Type Filter

1. Navigate to **Admin | Filters**.
2. Click **Create Filter**.



3. On the New Filter page, select the platform. For this example, select **Unix/Linux**.
4. From the **Filter Type** drop-down select **Advanced Commandline Filter**.
5. Enter a name and description and click **Create**.



6. Customize the newly created filter, click **Add Command**.

7. Select the matching type, Glob or RegEx. Use Glob for filename matches and RegEx for searches and matches of patterns in files.
8. Enter a **Command**.
9. Enter **Arguments**.
10. Enter a **Replacement**.
11. Click **Save Changes**.

Examples

A commandline filter examines the commandline (excluding the primary executable) and uses either Glob or RegEx for the pattern match. Here are examples for both options:

Example of Commandline Replacements

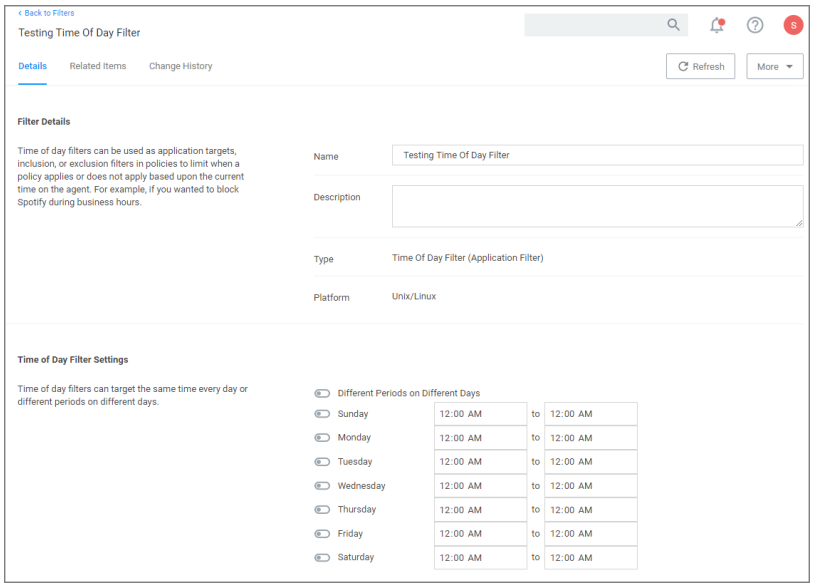
Command: `restart` Arguments: `pmagent` Replacement: `/usr/bin/systemctl restart pmagent` User submits: `sudo restart pmagent` Command executed: `/usr/bin/systemctl restart pmagent`

Limitations of the Advanced Commandline Filter

The command re-write is done BEFORE any action defined in the Policy, therefore commands that will also display actions assigned to the policy such as `runas user` and environment variable will not be displayed as expected, because the commandline filter is processed before the action.

Time of Day Filter

This type of filter exists to create policy parameters for specific time frames.



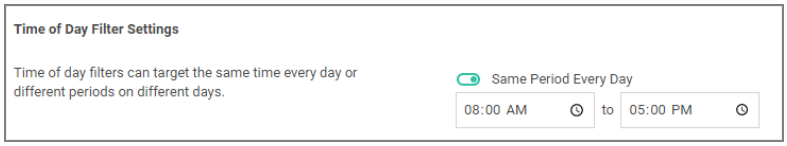
This filter is available for all supported platforms.

Parameters

The time of day filter has two different settings to allow you to set time and day allowances.

Flip the switch to toggle between these option:

- **Different Periods on Different Days** (default). When set to Different Periods on Different Days, the page also shows switches to turn on the time of day settings for the specific day of the week. By default no periods are enabled.
- **Same Period Every Day**, when turned ON only one period entry option is available



Save the changes after any customization.

Examples

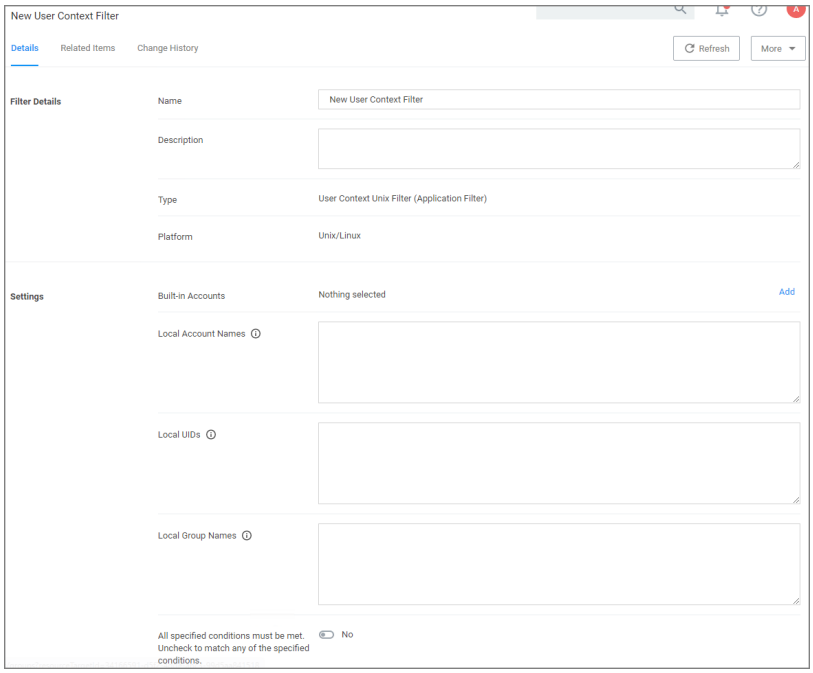
You can use the time of day filter in a policy to only pickup specific times or days of the week.

Using User Context Filters

User Context Filters are used in a policy as either an

- inclusion filter, to specify that the policy only applies to users in a specific AD Group.
- exclusion filter, to specify that the policy applies to everyone, except the users in a specific AD Group.

The User Context Filters are part of the Application Filter templates:



This filter is available for all supported OSs.

On-Premise

For Privilege Manager on-premises the **User Context Filter** can be used after the Active Directory synchronization completes. When creating and editing the filter, add any of the following information can be specified to identify the user context.

> **Note:** If you need to modify any items within Privilege Manager, duplicate the item and modify the duplicate instead of the built-in item so that an upgrade does not overwrite it.

- Built-in Accounts: Use **Add**, then select a resource and click **Select**.
- Local Account Names: If entering multiple account names, each entry must go on a new line.
- Local UIDs: If entering multiple UIDs, each entry must go on a new line.
- Local Group Names: If entering multiple local group names, each entry must go on a new line.
- Domain User Groups: Refer to "Leveraging the User Context Filter for NoMAD" topic below.

1. Select if **ALL** conditions must be met. Leave the box unchecked to match **ANY**. You can also specify if accounts must be enabled to be targeted. This is an important checkbox to set if specific users have been added.
2. Click **Save Changes** to save any customization of the filter.

Export Items

In Privilege Manager Administrators need the ability to export complete policies, including dependent filters, actions, resource targets and any related items. They also need the ability to then import those policies into another instance.

The export and import feature can be used for production environments with multiple instances and for troubleshooting purposes when assistance is needed.

The feature provides the ability

- to export single policies for specific troubleshooting purposes.
- to bulk export via policies folders at any given folder level, except on root folders, depending on specific needs.
- to choose to overwrite or leave in place what's already there.
- to select specific objects or bulk select

This feature supports the bulk migration and creation of policies, including all of their dependencies.

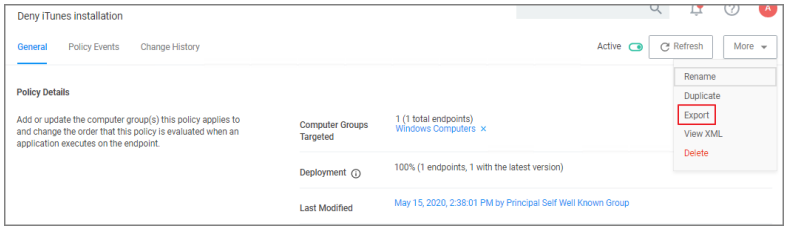
Exporting Items

Items at various levels of complexity can be exported. The UI offers several access points for an export operation.

Specific Policy Export

To export a specific policy with dependent filters and actions:

1. Navigate to the specific Policy and select it.
2. From the top-right **More** menu select **Export**.



3. A modal opens asking the user to confirm the download of the specific policy.

   Click **Download**.

   The policy is downloaded to your system's default download location as a .zip file

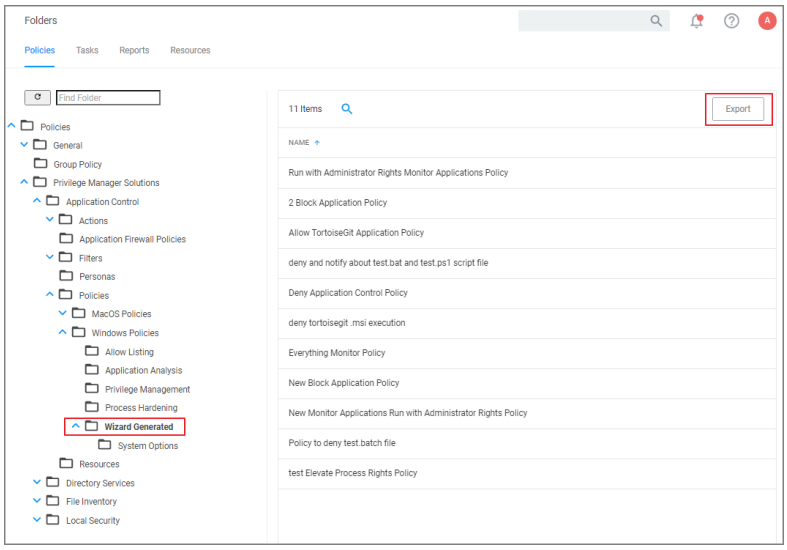
The policy details are downloaded in a zip file named after the policy name that was selected for export. The zip file contains one items.xml file with all the exported data. Extract the zip file and open/edit the exported xml.

The export of filters, tasks, or reports is done in a similar way, by navigating to the specific item, locating the Export button and proceeding through the export process steps.

Folder Exports

Bulk export of items is possible via the Folders page.

1. Navigate to **Admin | Folders**. The export of folders is available on the Policies, Tasks, and Reports. On the Resources tab, the export is only possible for Resource Filters.
2. From the folders tree select any of the available folders.



   Click **Export**.

3. A modal opens asking the user to confirm the download of the specific policy.

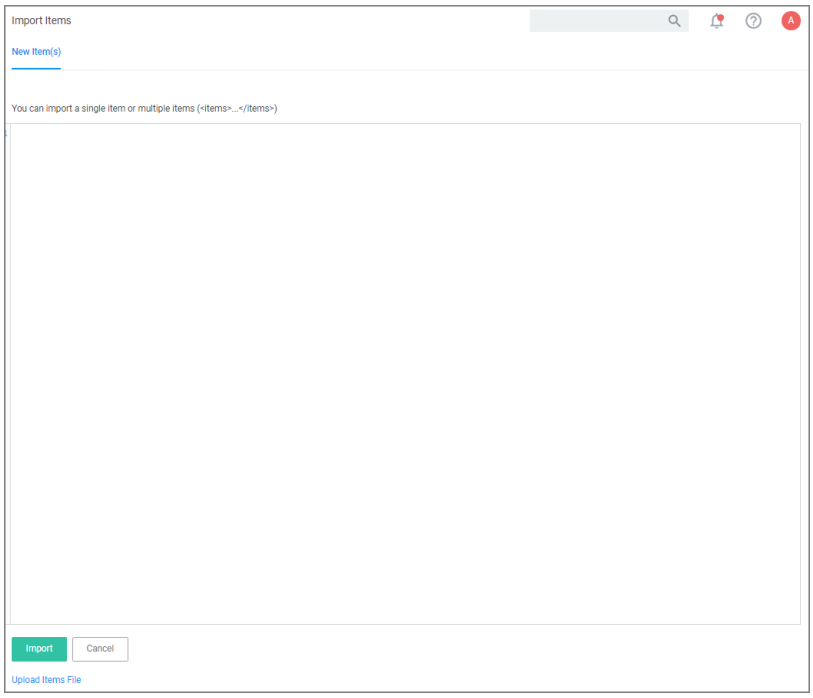
   Click **Download**.

The items are downloaded in a zip file named after the folder that was selected for export. The zip file contains one items.xml file with all the exported data. Extract the zip file and open/edit the exported xml.

Importing Items

Note: Prior to importing any data into your environment, Delinea recommends to create a backup of the current Privilege Manager Database.

Items can be imported in different ways, which are further detailed below.



Unsupported or missing file extensions trigger an error message on the import modal. The following file types are supported:

- .xml
- .zip

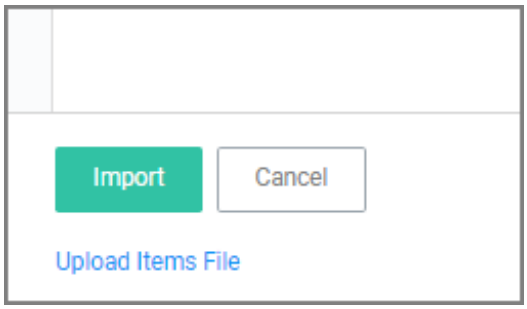
Using Import Items

1. Navigate to **Admin | Import Items**.
2. The xml viewer opens and you may copy xml item data here to import. Or use the **Upload Items File** option as described under Using Diagnostics Upload Items File.

Using Diagnostics Upload Items File

To import items via file upload follow these steps:

1. Navigate to **Admin | Diagnostics** and select **Import Items**.
2. Scroll to the bottom of the page and select the **Upload Items File** link.



3. The **Import Items** dialog opens, browse to your file location and select the file containing the data to import.

   Supported file types for the import are .xslt, .xbl, .xsl, .xml, and .zip.

   By default the **Overwrite Existing Items** checkbox is selected. If you want to skip items that already exist, uncheck the box. The import is based on the following conditions:

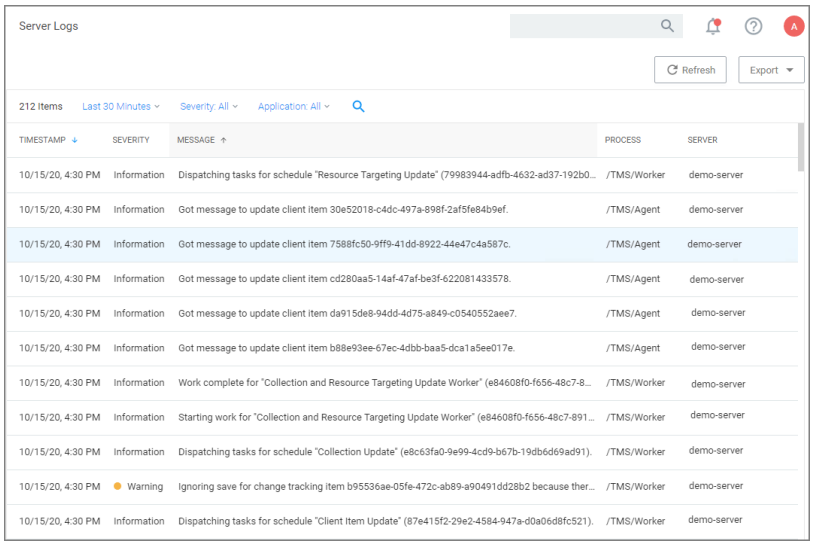
   - When the checkbox is selected, import all items (including changes saved in state).
   - When the checkbox is **NOT** selected, import only **new** items (including changes saved in state).
   - Any policies imported will be disabled (assuming they are not skipped).

4. Click the **Upload** button.

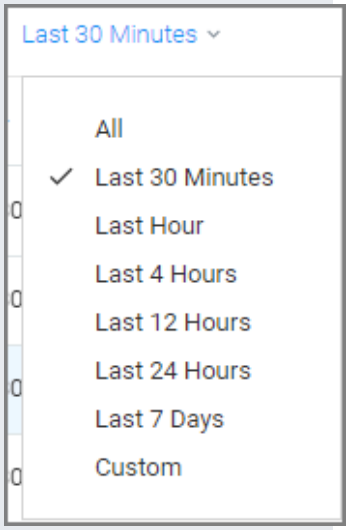
You can verify the uploaded data by navigating to **Admin | Folders**. Depending on your import, the data is listed under Policies, Tasks, or Resource Filters.

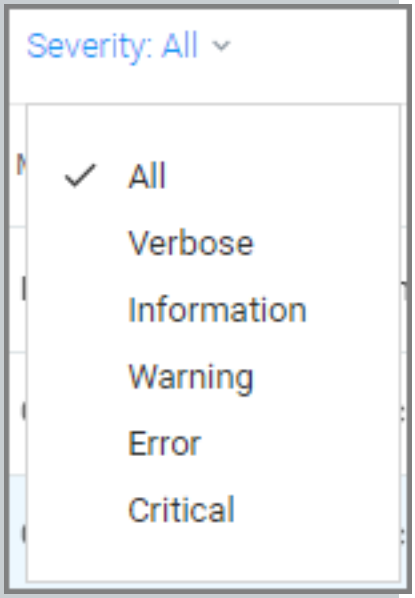
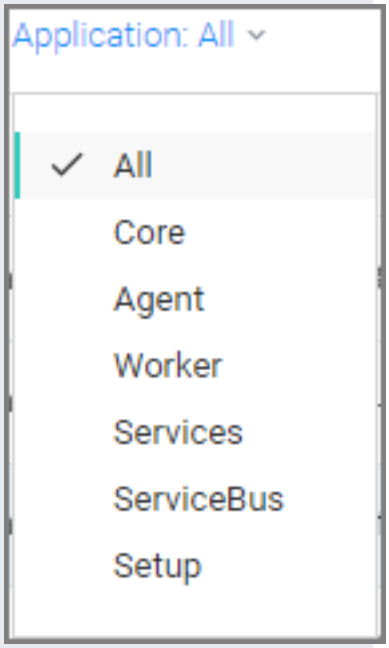
Server Logs

The Server Logs provide insight into the Privilege Manager Server Logs.



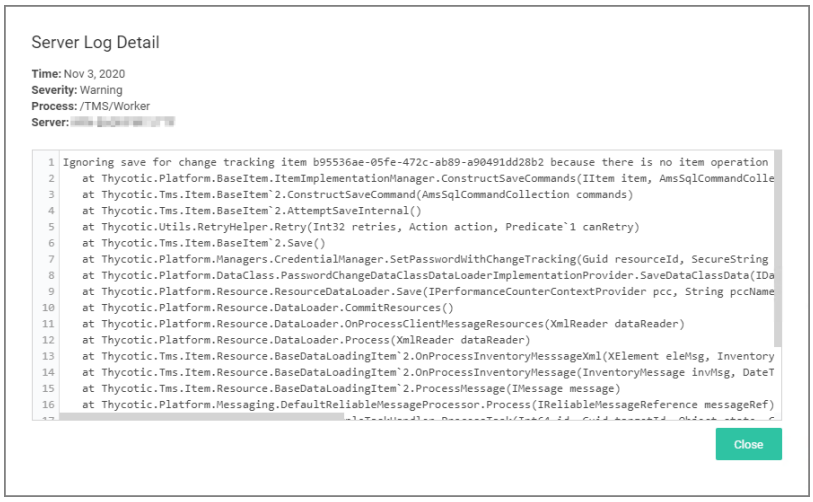
By default the Server Logs are shown for the last 30 minutes and with the Severity and Application set to All. These change be changed via the available drop-down options:

Drop-downs	Options
Duration	

Drop-downs	Options
Severity	
Application	

Details

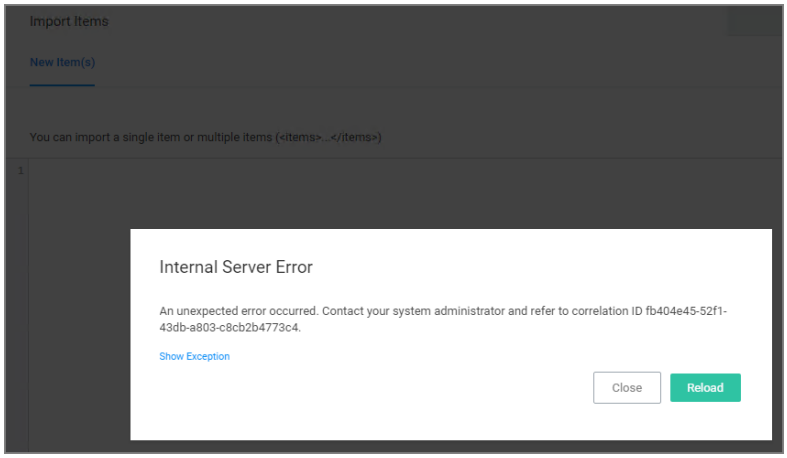
Details for a log entry can be viewed by clicking on the row containing the log entry.



Search by CorrelationID

The Server Logs are searchable via CorrelationID for better troubleshooting support. If you are looking for log details about an error that occurred in the UI, copy the CorrelationID from the error message and enter it in the table grid search field.

- Error providing CorrelationID:



- Search Server Logs for CorrelationID:

- Details for error based on CorrelationID search:

Personas

In Privilege Manager, Personas are collections of privileges for specific roles at an organization. You can assign Personas to users on a specific Computer Group to elevate their identity to perform specific tasks.

For example: A "SQL Administrator" Persona might be created that assigns rights to launch Certificate Manager and SQL Server Configuration Manager. Only users under this Persona would be allowed to execute these applications on your network.

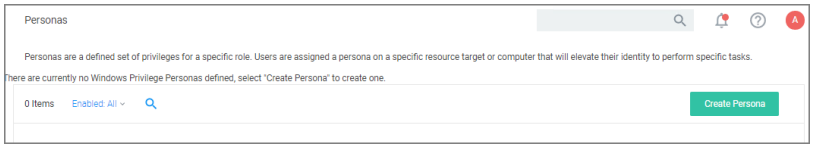
Note: It is recommended to setup Active Directory Synchronization first and run the synchronization task to then easily assign Personas to domain user groups.

Viewing your Personas

To see all your Personas navigate to **Admin | Personas**. From the Windows Privilege Personas page, you can create new Personas and manage existing Personas.

Creating a Persona

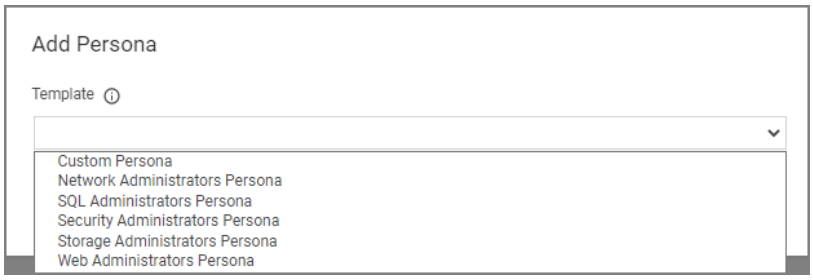
To create a Persona, click **Create Persona**. You will be presented with a dropdown list of Persona Templates to choose from.



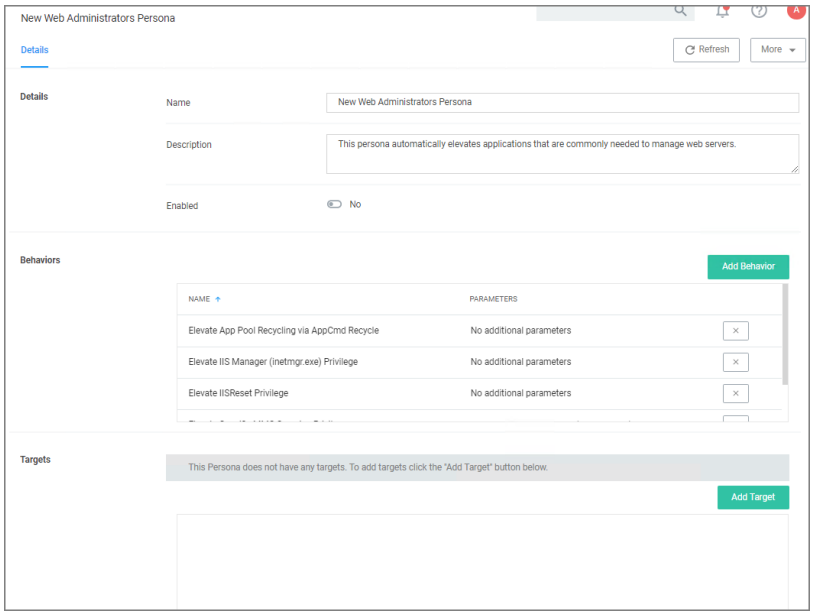
Personas Template	Description
Custom Persona	An empty Persona template for the users to customize based on their needs.

Personas Template	Description
Network Administrators Persona	Automatically elevates applications that are commonly needed to manage network configurations. Elevate DHCP, DNS, and NLB Configuration
Security Administrators Persona	Automatically elevates applications that are commonly needed to manage local users and security settings. Elevate Local User and Groups and Group Policy Object Editor
SQL Administrators Persona	Automatically elevates applications that are commonly needed to manage SQL servers. Elevate Certificate Manager, ODBC Configuration, and SQL Server Configuration Manager
Storage Administrators Persona	Automatically elevates applications that are commonly needed to manage file storage settings. Elevate Disk Defragmentation, Disk Management, ISCSI Connection Configuration, Quota Management, Shared Folders, and Windows Backup
Web Administrators Persona	Automatically elevates applications that are commonly needed to manage web servers. Elevate App Pool Recycling, Certificate Manager, IISReset, and adding TCP Firewall Rules

Select a Persona Template and then provide a Name and Description. Once you are ready to proceed, click Create. If you selected any Persona Template other than Custom Persona then you will have pre-populated Behaviors that you can choose to delete or keep. Otherwise, you will start with a blank Persona.



For Persona Settings, you can change the name, description, and whether the Persona will be enabled. For Persona Behaviors, you can click Add Behavior and choose which privilege(s) you want to allow for this Persona. Finally, for Persona Targets you can choose which Active Directory Domain User Groups this Persona will affect and on which Active Directory Organizational Units this Persona will apply.



Set the persona to **Enabled** and click **Save Changes** to finish creating your Persona.

Resource Explorer

Resource Explorer provides information about any type of resource item in Privilege Manager.

> **Note:** If you need to modify any items within Privilege Manager, duplicate the item and modify the duplicate instead of the built-in item so that an upgrade does not overwrite it.

Resource Explorer provides:

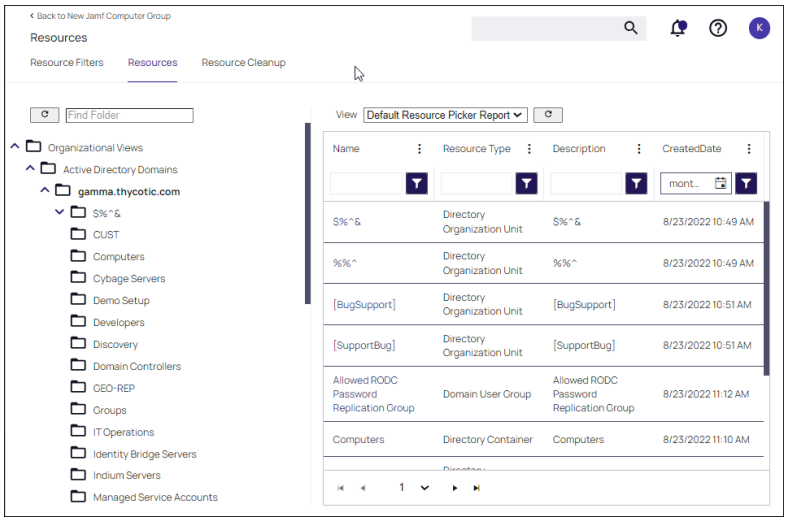
- **Summary**, which contains general information, such as name, description, and modified date for any resource accessed.
- **Known Data**, such as any data known that relates to the resource. This data is different from resource type to resource type. For example, a domain has Global Domain Details and no account details, and a file will have all sorts of information pertaining to the file.
- **Events** are log-style data entries that are directly related to the resource. For example for discovered files, those are the events that are reported from and endpoint.
- **Associations**, are any associated/related items.

Resources can be deleted from the Resource Explorer page.

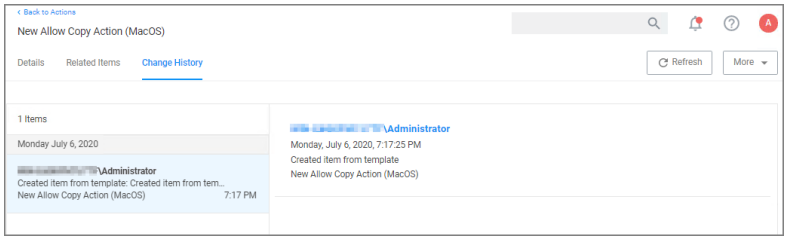
> **Note:** Only use Delete when you are absolutely sure that you want to delete that resource. Clicking on Delete will delete the current resource record you are viewing.

Resource Explorer is accessible by either navigating to:

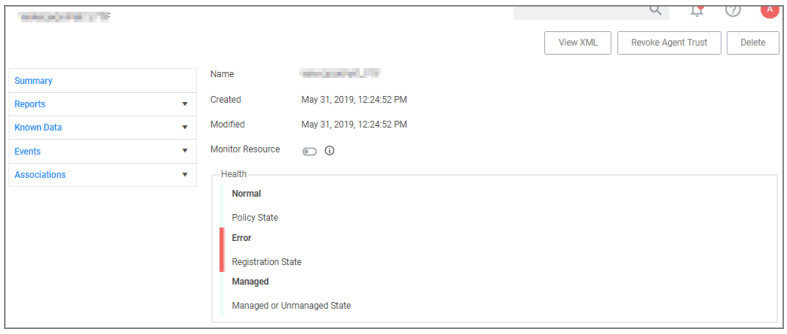
- **Admin | Resources** and expanding the Resources tree drilling down to a named resource to further explore and/or edit.



- **Change History** tab of a named resource.



- any named item, such as a report, in the Privilege Manager console and selecting a named resource. Example navigation for the following image, *Admin | Agents | select one system from the list | select one computer from "Managed Computers by Operating System " list*:



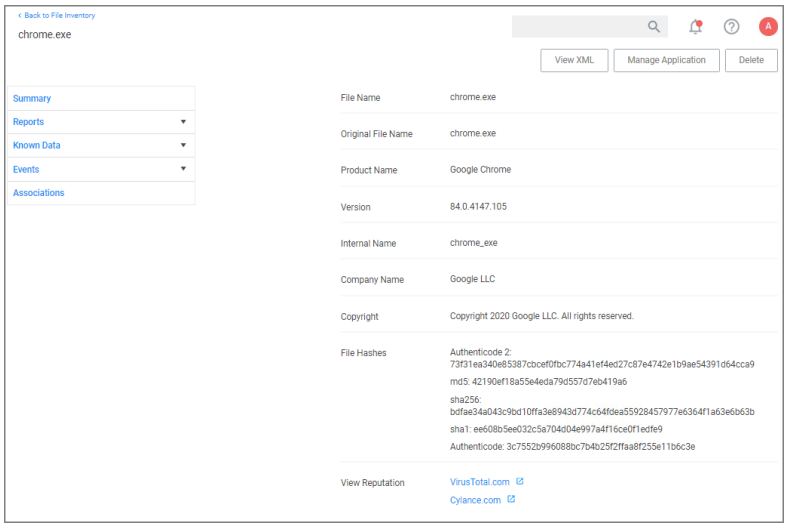
Example for Discovered Files

You enter the Resource Explorer for discovered files through **File Inventory** on the main navigation tree. On the Events page, click any of the discovered files and use **View File** to drill down to the files resources.

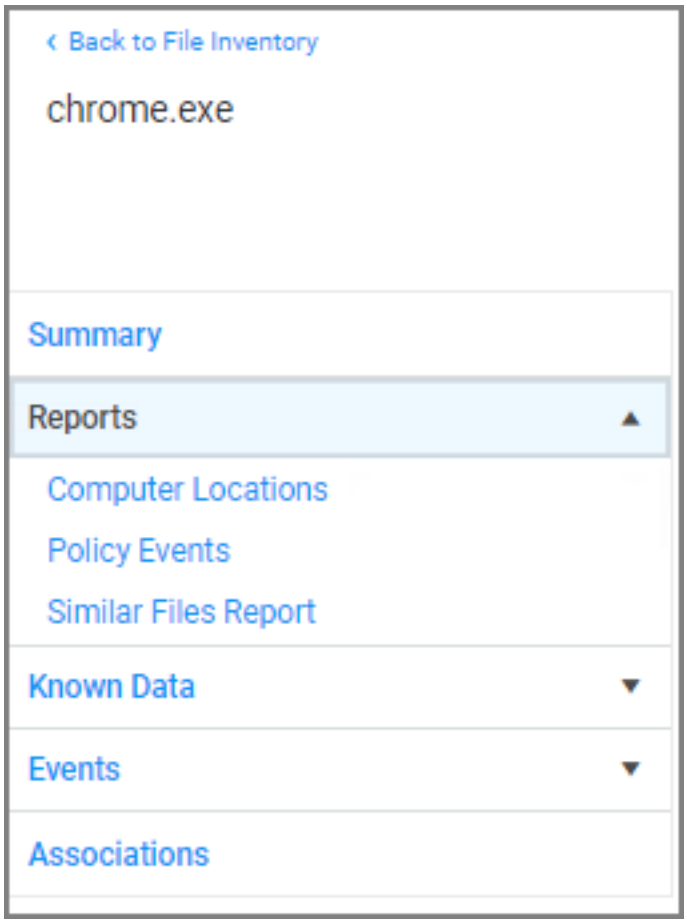
The following image shows all discovered information about the chrome.exe file, such as:

- File Name
- Original File Name

- Product Name
- Version
- Internal Name
- Company Name
- Copyright information
- File Hashes
- View Reputation, if a reputation provider is integrated with your Privilege Manager instance.



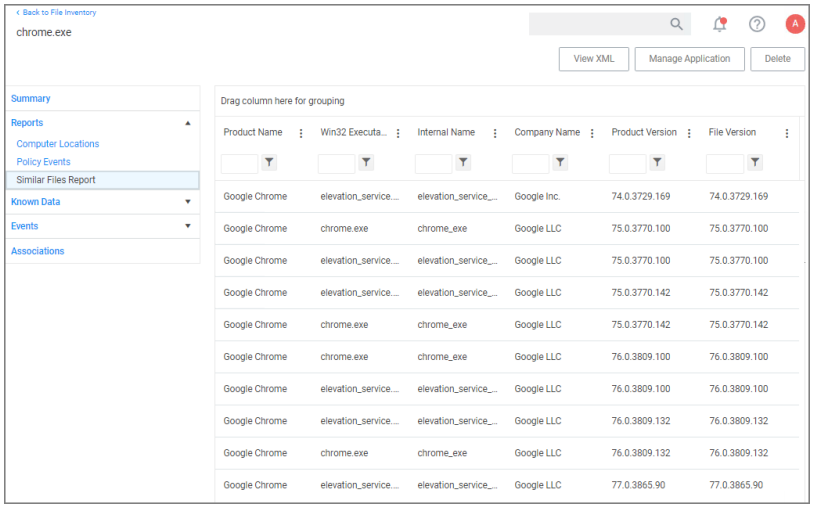
Under the **Reports** drop-down you can look at further details on the **Computer Locations**, **Policy Events**, and **Similar Tiles Report** tabs.



The **Computer Locations** tab provides details about the discovery locations where the file was discovered.

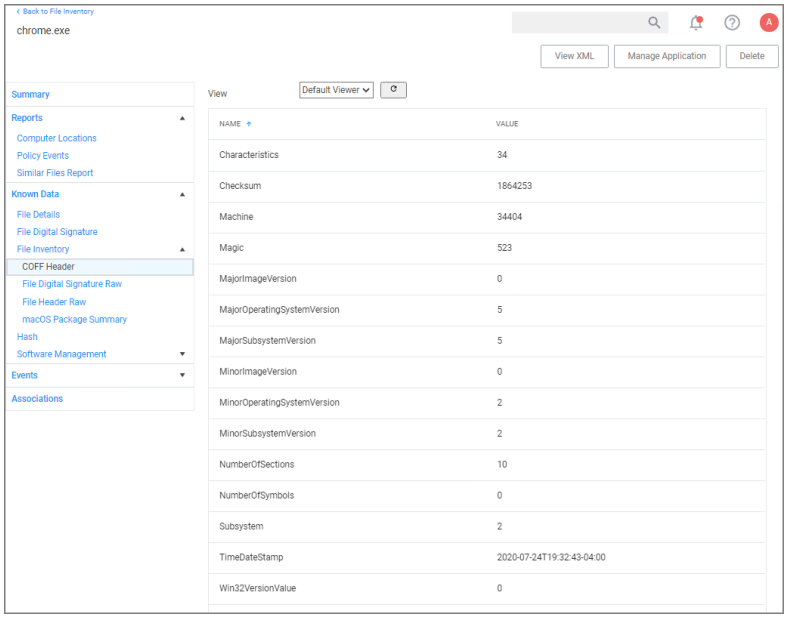
The **Policy Events** tab provides details about the policy events that triggered by the file if executed.

The **Similar Files Report** tab provides a list of and links to similar files that have been discovered by Privilege Manager.

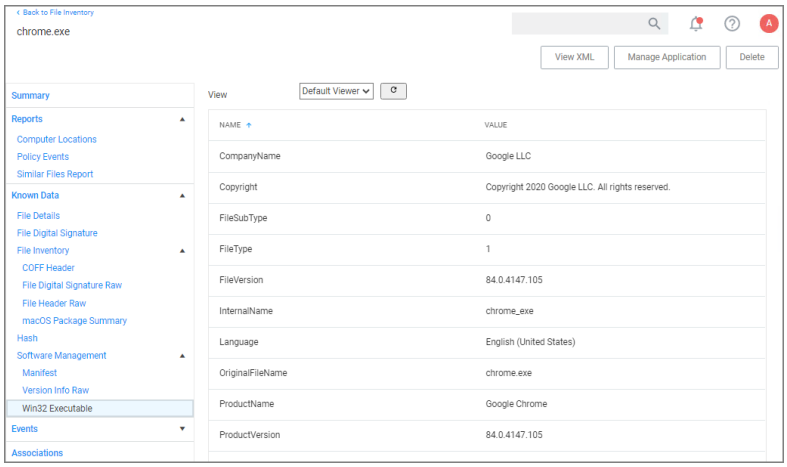


The Known Data for a discovered file includes details like:

- File Inventory, which provides COFF Header and File Digital Signature data in raw form.

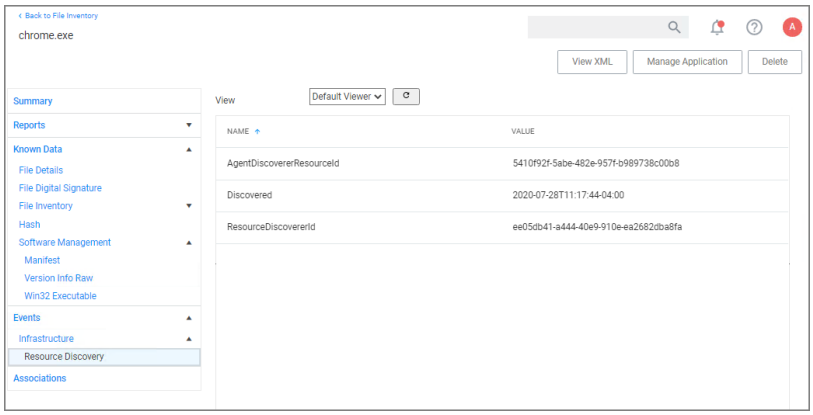


- Software Management, which provides the files Manifest, Version Info in raw form, and Win32 Executables details.



- File Details, such as name, file extension, file size, and if protected or not.
- File Digital Signature, which provided information on the Signer, Countersigner if available, and the signature date/time stamp.
- Hash, provides details on the name, the hash, and hex hash.

Under Events, Infrastructure offers a view into the Resource Discovery events that discovered the file, in this example the File Agent Discoverer and File Agent Discoverer (File Location) events.

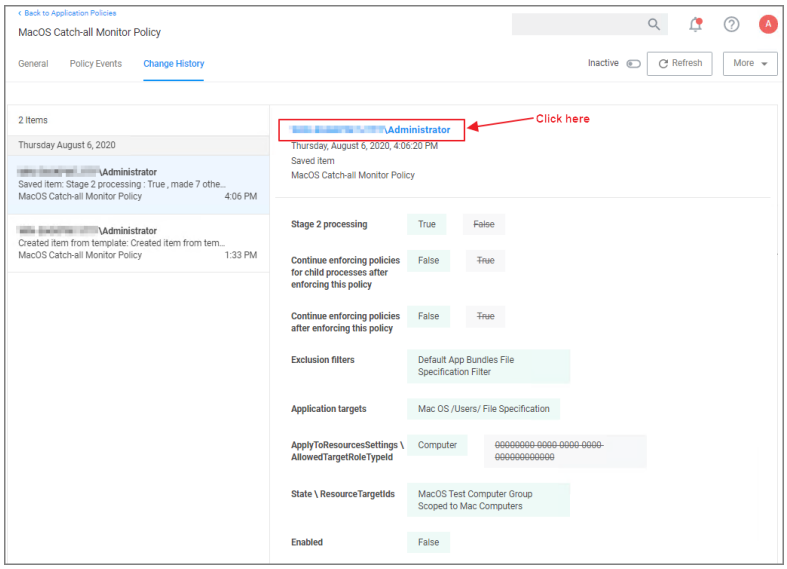


This discovered file resource has no related items associated and thus the Associations area of the Resource Explorer is empty.

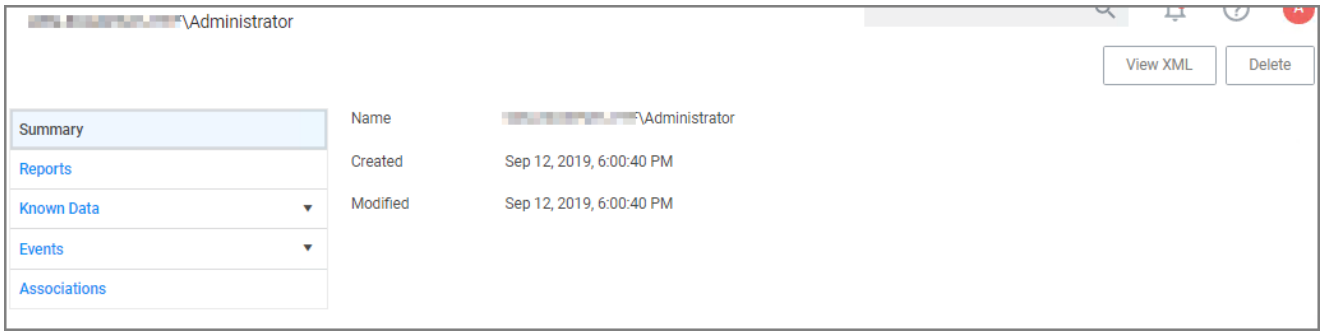
Example for User Resource

When you are looking at change history for any item and click the view user link, you access the **Resource Explorer** for that specific user resource. The Summary information for that specific user resources shows:

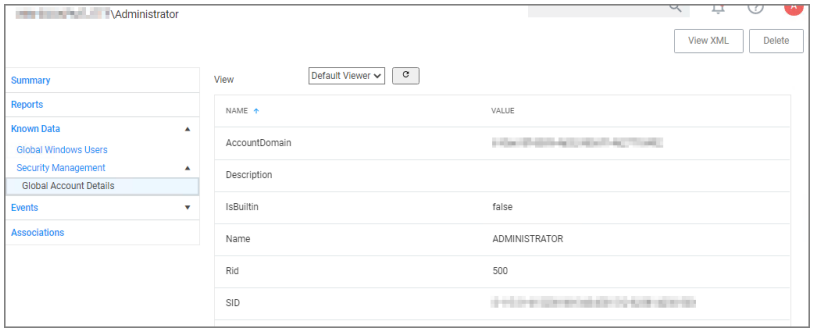
- Name – this is the user account that made the change.
- Created – indicates when the item was created.
- Modified – indicates when the item was last modified.



The resource explorer is providing information about the current state of that user resource.



Under **Known Data** we can explore the information for **Security Management | Global Account Details**.

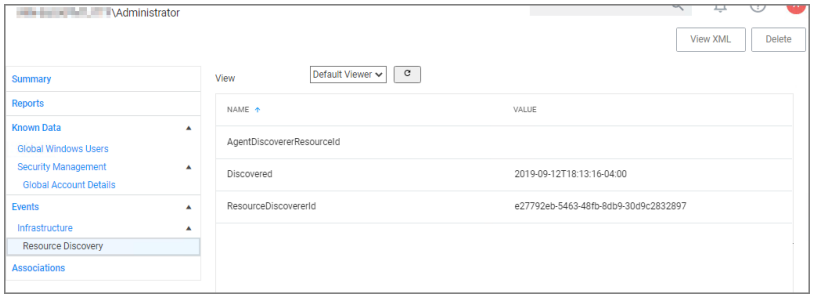


Users can select the View from the drop-down and see information on the type of the resource. User resources provide details about:

- AccountDomain - identifies the domain for the user account.
- Description
- IsBuiltin - can be true false to indicate if the account in built-in or not.
- Name - Name associated with the user account.
- Rid
- SID

Selecting the Global Windows Users information shows Name, Domain, and UserId.

Under **Events**, you can view **Infrastructure | Resource Discovery** information:



Under **Associations** you can see related items, such as **Group Membership**, which is based on the users credentials.

Error Message after Deleting a User Resource

In case a resource was deleted, an error message like the following will be shown the next time the resource view link is accessed.

InvalidItemIdException
The server could not find an item required for this request. Please check the server logs for additional information.
The specified Guid '9c0f4d76-5557-4aab-941d-3d13bc30cf81' is not a valid Item.

Computer Name Pattern Collections

If you have specific patterns of computer names that you wish to target, create a query-based collection using the **Computers by Name Patterns Query**. This collection can then be used within Computer Group definitions. The query uses SQL wildcard characters in the search to create a custom collection based on the results.

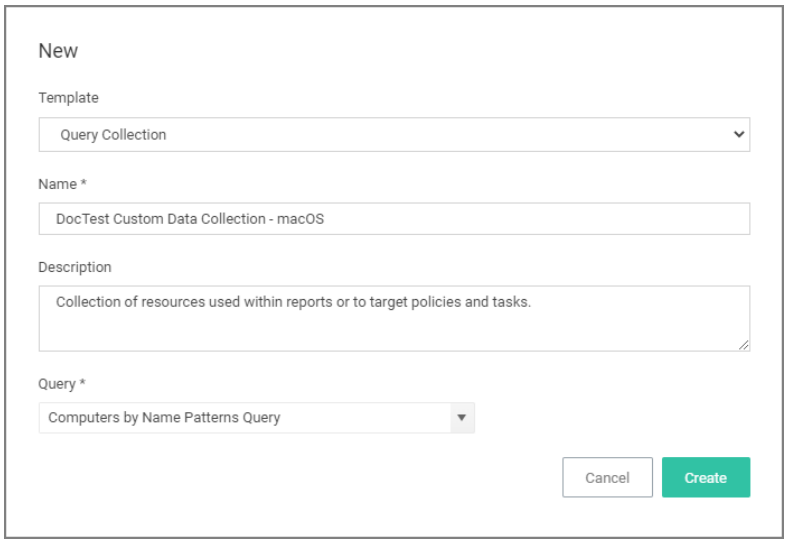
For example, if a company has their computer resources around the globe set up to have geo location references like EU, AS, US, etc. as a pre- or postfix, collections can be created for all machines in either Europe, Asia, or the United States based on those characters in the computer names.

The query for creating a custom data collection is **Computer by Name Pattern Query**, which is available for macOS, Unix/Linux, and Windows collections.

Creating a Computer Name Pattern Collection Query

These queries are dependent on the admin role a user might have. Privilege Manager Administrators can create new collections on the **Collections** root level. Privilege Manager macOS, Unix/Linux, or Windows Administrators must select the OS specific folder from the **Collections** tree.

1. Navigate to **Admin | Resources** and select the **Resource Filters** tab.
2. From the **Resource Filters** tree, select **Collections**.
3. Click **Create**.
4. From the **Template** drop-down, select **Query Collection**.
5. Enter a name and edit the description to better identify the purpose of the resource you are creating.
6. From the **Query** drop-down, select **Computer by Name Pattern Query**.



7. Click **Create**.
8. Select **Filter Definition**.
9. In the **Computer name patterns** field, enter one or more comma-separated computer name patterns.

   For example, *EU-%,%123,SRV-%01*

   - would select all computers that started with *EU-*,
   - include all computer names that end with *123*,
   - and all that start with *SRV-* but must end with *01*.
10. Click **Save Changes**.
11. Select **Membership**.
12. Click **Update Membership** to immediately run the **Collection and Resource Targeting Update** task. This task is assigned to a shared schedule "Collection Update", which runs every 15 minutes by default.

Using the Query for a New Computer Group

To create a new computer group using the new custom collection query, follow these steps:

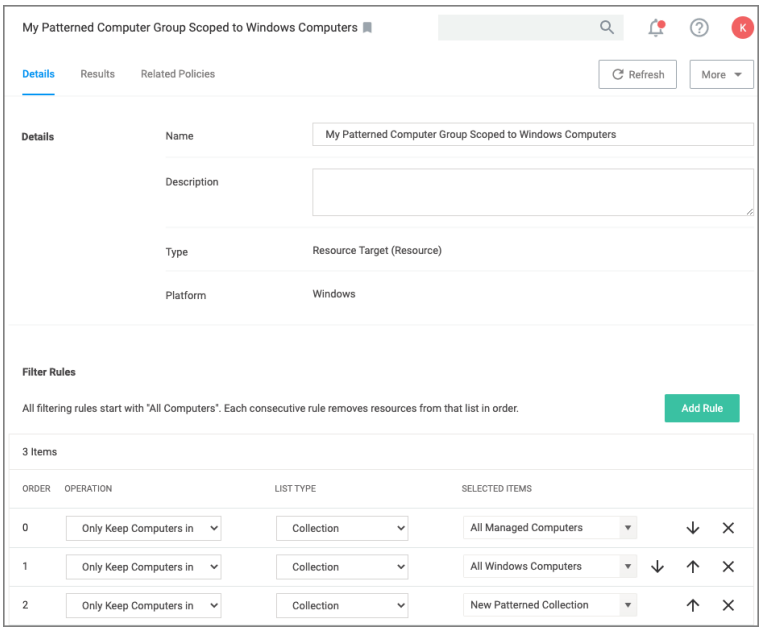
1. Navigate to **Computer Groups**, click **Create Computer Group**.
2. From the Platform drop-down select the targeted platform for your new group.
3. Enter a Name and Description for your new computer group.
4. Click **Create**.
5. Under **Filter Rules**, click **Add Rule** to add another rule (leave the existing platform-based rule at the top). For the new rule, specify for:

   a. **Operation** drop-down, select **Only Keep Computers in**.

   b. **List Type** drop-down, select **Collection**.

c. **Selected Items** drop-down, select the **All Managed Computers**.

6. Click **Add Rule** again to add another rule (leaving the existing rules in place). For this new rule specify for:
   a. **Operation** drop-down, select **Only Keep Computers in**.
   b. **List Type** drop-down, select **Collection**.
   c. **Selected Items** drop-down, select the *Computer Name Pattern Collection Query* you created above.



7. Click **Save Changes**.

Computer by Name Filter

For computer groups that do not employ Active Directory services to identify computers, the Filter by Name filter rule can be used to identify computers using any of three identification methods:

- manual entry
- copy from a spreadsheet
- populate and manage from an API

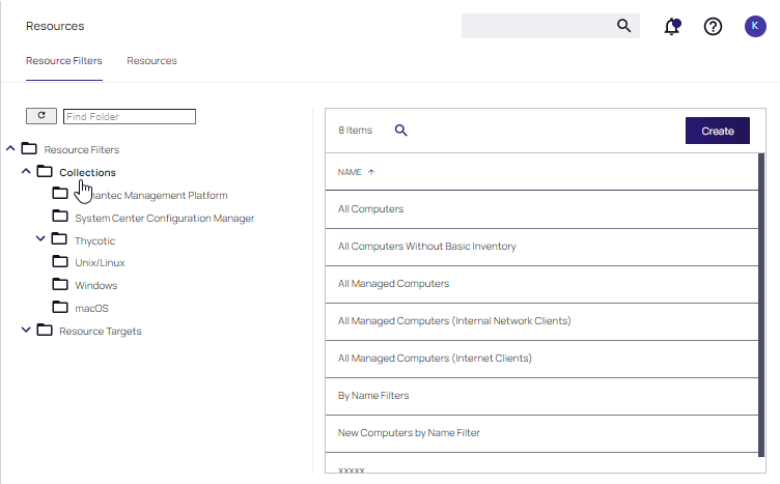
These instructions step through the Filter by Name feature that is used to create filters for computer groups using computer names.

Creating a Computer Name Filter Collection Query

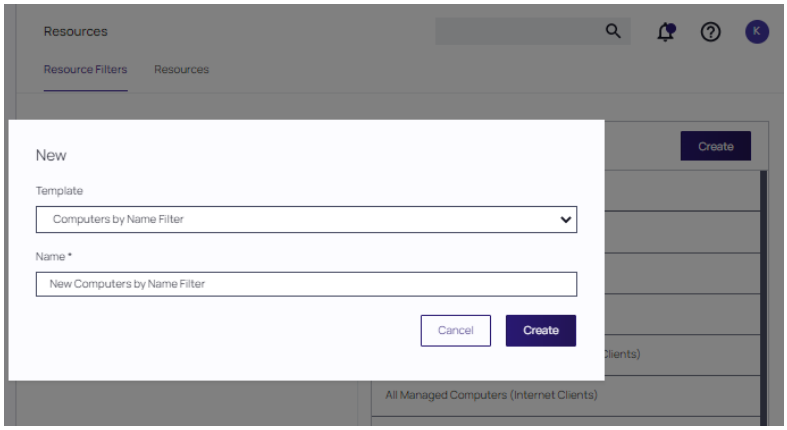
These queries are dependent on the admin role a user might have. Privilege Manager Administrators can create new collections on the **Collections** root level. Privilege Manager macOS, Unix/Linux, or Windows Administrators must select the OS specific folder from the **Collections** tree.

1. Navigate to **Admin | Resources** and select the **Resource Filters** tab.
2. From the **Resource Filters** tree, select **Collections**.

3. Click **Create**.



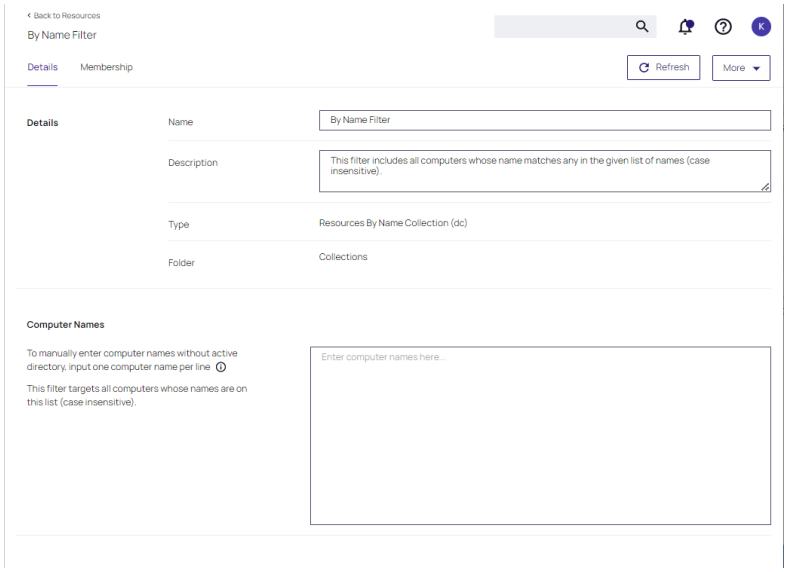
4. From the **Template** drop-down, select **Computers by Name Filter**.
5. Enter a name and edit the description to better identify the purpose of the resource you are creating.



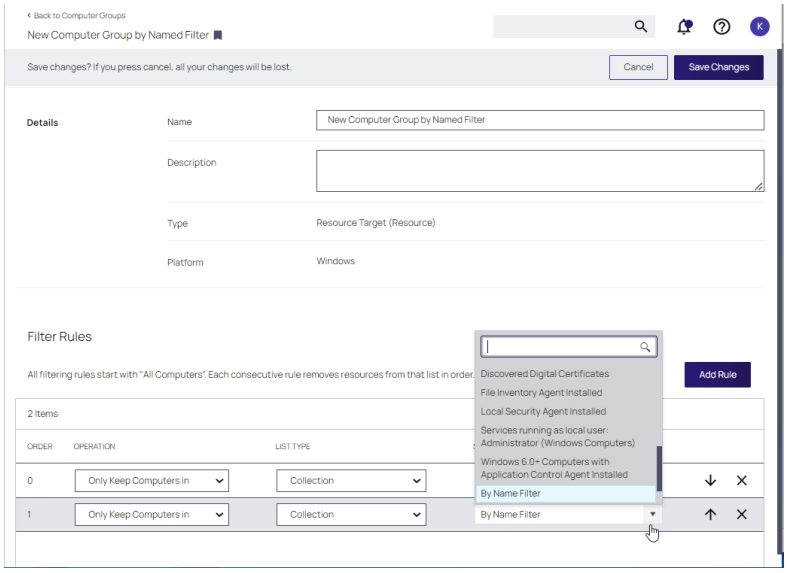
6. The Details page for the newly created collection is displayed. Three options are available for entering names in the **Computer Names** field: enter names manually, paste in entries from an Excel spreadsheet, or use the API to populate names.

   To use the API method, refer to the instructions for Populating Computer Names using the API after these

instructions. Proceed to create a rule for the named filter in the designated computer group next.



7. Navigate to the Computer Group that will be associated with the newly created filter.
8. On the Details page for that computer group, click **Add Rule**.
9. Specify a **Collection** as the **LIST TYPE**. Select the newly created filter in the **SELECTED ITEMS** drop-down.
10. Click **Save Changes**.



11. Proceed with the instructions for Populating Computer Names using the API.

Populating Computer Names using the API

Below is an **example** of a PowerShell script that is used to populate computer names.

To create your script, use the By Name Filters methods presented in the Privilege Manager API.

Note: The API script can be run at your discretion at any time computer names need to be refreshed.

Example PowerShell Script

The example PowerShell script incorporates API methods that includes `Create-ComputersByNameFilter`. In practice, this is not required for subsequent script executions. Instead, use one of the API mthods to update the list and `get $filterId` from the item ID shown in the browser URL when viewing the **Computers by Name** filter created in the first step.

In this example,

- `$api_user_clientid` and `$api_user_secret` are obtained from the **Admin** | **Users** page for that user.
- `client ID` and `secret` are obtained from the Details page for that user.

```
# Computers By Name Filter Test Script #
$api_user_clientid = ''
$api_user_secret = ''
$tmsBaseUri = 'https://localhost/Tms'
$tmsAPIBaseUri = "$tmsBaseUri/services/api"
$tmsAPIAuthUri = "$tmsAPIBaseUri/logon/token"
$tmsAPIByNameFiltersUri = "$tmsAPIBaseUri/v1/bynamefilters"
$tmsAPIContentType = 'application/json'
$tmsAPIBearerToken = $null;
# Functions
function Ignore-SSLCertificateErrors
{
    if (-not
([System.Management.Automation.PSTypeName]'ServerCertificateValidationCallback').Type)
    {
        $certCallback = @"
            using System;
            using System.Net;
            using System.Net.Security;
            using System.Security.Cryptography.X509Certificates;
            public class ServerCertificateValidationCallback
            {
                public static void Ignore()
                {
                    if(ServicePointManager.ServerCertificateValidationCallback ==null)
                    {
                        ServicePointManager.ServerCertificateValidationCallback +=
                            delegate
                            (
                                Object obj,
                                X509Certificate certificate,
                                X509Chain chain,
                                SslPolicyErrors errors
                            )
                            {
                                return true;
                            };
                    }
```

```
                }
            }
"@
        Add-Type $certCallback
    }
    [ServerCertificateValidationCallback]::Ignore()
}
function Read-ResponseJson
{
    param ([Microsoft.PowerShell.Commands.WebResponseObject] $response)
    if($response.StatusCode -lt 200 -or $response.StatusCode -gt 299)
    {
        throw "Request failed with error code: $($response.StatusCode):
$($response.StatusDescription)"
    }
    ConvertFrom-Json $response.Content
}
function Authenticate-APIUser
{
    if($tmsAPIBearerToken -eq $null)
    {
        $body = "{ ""username"": ""$api_user_clientid"", ""password"": ""$api_user_
secret"" }"
        $response = Invoke-WebRequest -Uri $tmsAPIAuthUri -Body $body -ContentType
$tmsAPIContentType -Method Post
        $tmsAPIBearerToken = Read-ResponseJson -response $response
    }
    $tmsAPIBearerToken
}
function Invoke-APIRequest
{
    param ([string]$uri, [string]$body, [Microsoft.PowerShell.Commands.WebRequestMethod]
$method)
    $bearerToken = Authenticate-APIUser
    $headers = @{Authorization="Bearer $bearerToken"}
    if(-not $body)
    {
        $response = Invoke-WebRequest -Uri $uri -Method $method -Headers $headers
    }
    else
    {
        $response = Invoke-WebRequest -Uri $uri -Method $method -Body $body -ContentType
"application/json" -Headers $headers
    }
    Read-ResponseJson -response $response
}
function Create-ComputersByNameFilter
{
    param ([string]$name, [string]$description, [string]$names)
    $body = "{ ""Name"": ""$name"", ""Description"": ""$description"", ""Names"":
""$names"" }"
    $response = Invoke-APIRequest -uri "$tmsAPIByNameFiltersUri/new" -body $body -method
Post
```

```
    $response
}
function Add-ComputersByNameToFilter
{
    param ([Guid]$filterId, [string]$names)
    $body = "{ ""Names"": ""$names"" }"
    $response = Invoke-APIRequest -uri "$tmsAPIByNameFiltersUri/$filterId/add-names" -body
$body -method Post
    $response
}
function Remove-ComputersByNameToFilter
{
    param ([Guid]$filterId, [string]$names)
    $body = "{ ""Names"": ""$names"" }"
    $response = Invoke-APIRequest -uri "$tmsAPIByNameFiltersUri/$filterId/remove-names" -
body $body -method Post
    $response
}
function Set-ComputersByNameToFilter
{
    param ([Guid]$filterId, [string]$names)
    $body = "{ ""Names"": ""$names"" }"
    $response = Invoke-APIRequest -uri "$tmsAPIByNameFiltersUri/$filterId/names" -body
$body -method Post
    $response
}
function Get-ComputersByNameFromFilter
{
    param ([Guid]$filterId)
    $response = Invoke-APIRequest -uri "$tmsAPIByNameFiltersUri/$filterId/names" -body
$body -method Get
    $response
}
function Get-ComputersByNameFromFilterAsCsv
{
    param ([Guid]$filterId)
    $response = Invoke-APIRequest -uri "$tmsAPIByNameFiltersUri/$filterId/namescsv" -body
$body -method Get
    $response
}
function Get-ComputersByNameFromFilterAsLines
{
    param ([Guid]$filterId)
    $response = Invoke-APIRequest -uri "$tmsAPIByNameFiltersUri/$filterId/namesnewline" -
body $body -method Get
    $response
}
Ignore-SSLCertificateErrors
# Create a new filter
$response = Create-ComputersByNameFilter -name "Test Computers by Name From API" -
description "This is a test - delete me" -names 'Computer1, Computer2, Computer3'
$filterId = $response.Result
# Add some new names
```

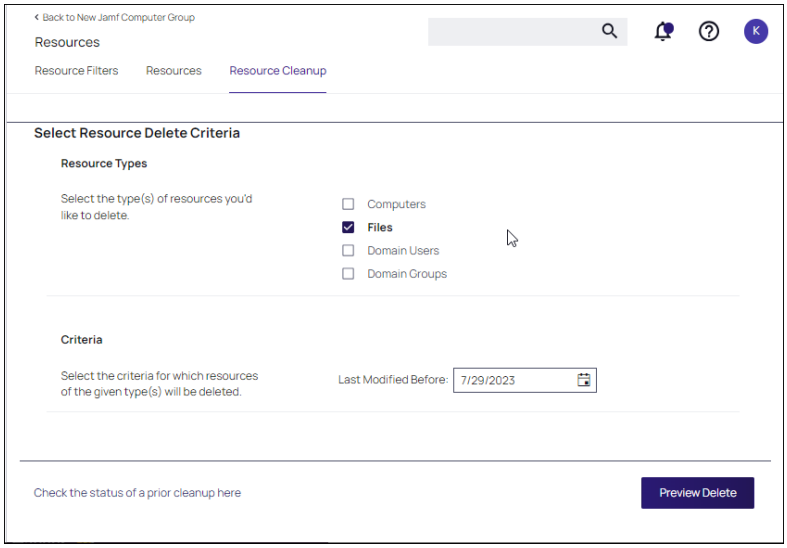
```
Add-ComputersByNameToFilter -filterId $filterId -names 'Comp4\r\ncomp5'
# Remove some names
Remove-ComputersByNameToFilter -filterId $filterId -names 'Computer1,Computer2'
# Show current names
Get-ComputersByNameFromFilter -filterId $filterId
# Set the full list of names (overwrite)
Set-ComputersByNameToFilter -filterId $filterId -names 'New1, NewABC'
# Show current names
Get-ComputersByNameFromFilter -filterId $filterId
# Show current names as CSV
Get-ComputersByNameFromFilterAsCsv -filterId $filterId
# Show current names as one name per line
Get-ComputersByNameFromFilterAsLines -filterId $filterId
```

Resource Cleanup

Resource Cleanup removes resources, based on the last modified date. The resources available to be deleted are Computers, Files, Domain Users and Domain Groups.

> **Note:** **Resource Cleanup** is limited to 200,000 items per the time frame criteria. If 200,000 items are exceeded, only the first 200,000 will be processed.

1. Navigate to **Admin** | **Resources**. At the Resources page, select **Resource Cleanup**.
2. Select the **Resource Types** and **Criteria** for cleanup.



3. Select **Preview Delete**.

> **Note:** Deleting a large number of files (>10,000) impacts the size of the SQL Server Database Transaction Log. Maintenance may be required.

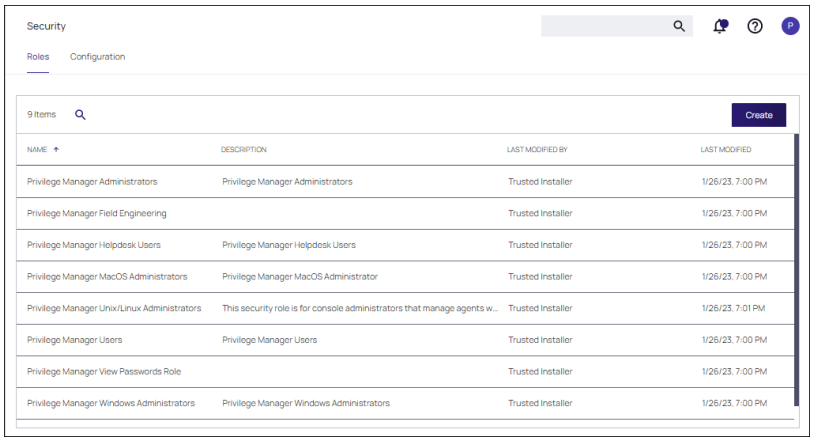
4. After confirming the resources to be deleted, select **Start Delete**.

Note: Resources will not be deleted if other items depend on them, even if they are shown in the Preview list.

Security

Roles Tab

The following Privilege Managerroles are available by default and it is possible to add to or remove members from these roles. Privilege Manager also allows the creation of new roles, if a customer environment requires more role support.



Privilege Manager's Roles logic prevents the removal of a user account with an Administrator Role, if that user account is the last with those Administrator Role privileges. Privilege Manager does not allow current users to delete their own account.

Privilege Manager manages the roles of users accessing the console, unless Privilege Manager is connected to Secret Server. When connected to Secret Server, role membership is controlled by Secret Server.

Also refer to the following topic: User Credentials and Roles.

All these roles are considered application role permissions.

Privilege Manager Administrators

This role allows the Privilege Manager Administrator to have full administrative access to the Privilege Manager Server Console.

Privilege Manager Field Engineering

This role is reserved for future use.

Privilege Manager Helpdesk Users

This role allows the user to have approve or deny escalation requests access. The helpdesk role can also disclose passwords.

Privilege Manager macOS Administrators

This role allows the Privilege Manager macOS Administrator to have full administrative access to the Privilege Manager Server Console to administer local security and application control items pertaining to macOS systems. This role can view but not edit Unix/Linux and Windows policies.

Privilege Manager Unix/Linux Administrators

This role allows the Privilege Manager Unix/Linux Administrator to have full administrative access to the Privilege Manager Server Console to administer local security and application control items pertaining to Unix/Linux-based endpoints. This role can view but not edit macOS and Windows policies.

Privilege Manager Users

This role allows the user to have read permissions to most items, but no rights to modify security permissions. This role can disclose passwords.

Privilege Manager View Password Role

This role allows the user to have view access to passwords for managed users in Privilege Manager. They can view the current passwords and password change history.

Privilege Manager Windows Administrators

This role allows the Privilege Manager Administrator to have full administrative access to the Privilege Manager Server Console to administer local security and application control items pertaining to Windows systems. This role can view but not edit macOS and Unix/Linux policies.

Creating a Role

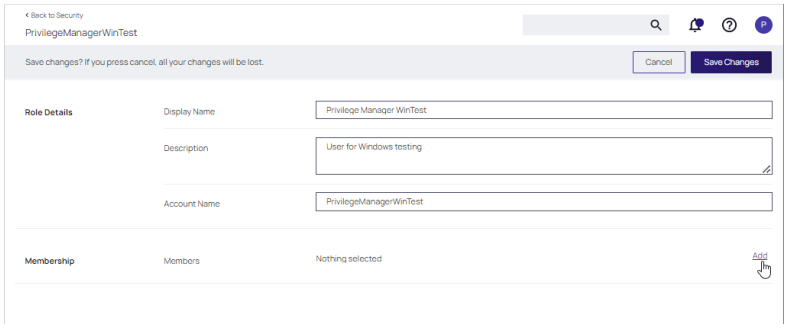
1. On the top of the Roles page, click **Create**.
2. Enter a **Role account name** and click **Create**.

   Note: Although spaces are not allowed in the role account name, spaces and special characters can be used in the display name after the role is created.

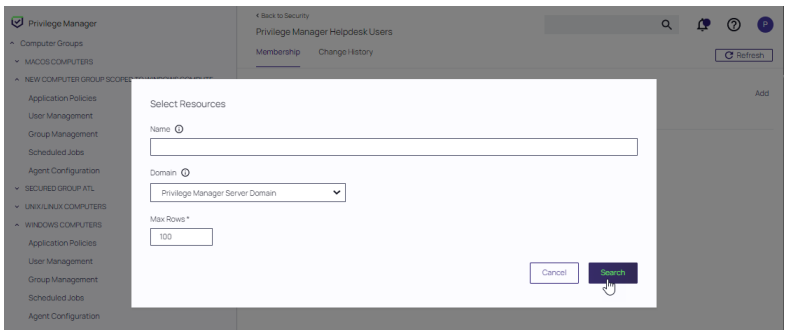
3. The new Role page opens, where you can add or edit the **Display Name**, **Description**, or **Account Name**.

Note: Only the display name and description can be changed when the role is created. Account Name is read-only.

4. Add Users, or any resource, to the role. Click **Add**.



a. At the **Select Resources** dialog, identify users and groups that will be added to the role. You can enter a name, partial name, or leave it empty to find all. Click **Search** and then select the users and groups to be added to the role.



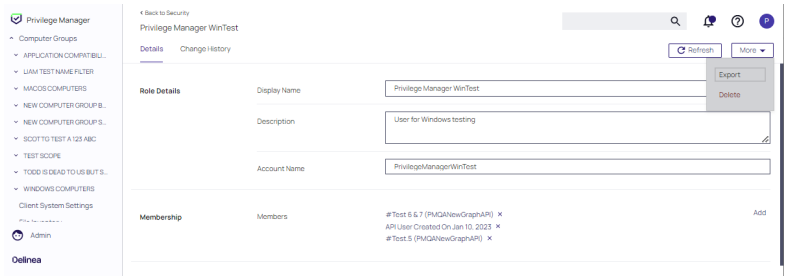
b. Available users/groups are displayed. Enable the check boxes for resources to add and click **Select**. Confirm your selections and click **Save Changes** when prompted.

The selected resources appear in the **Membership** portion of the page.

Editing, Deleting, and Exporting a Role

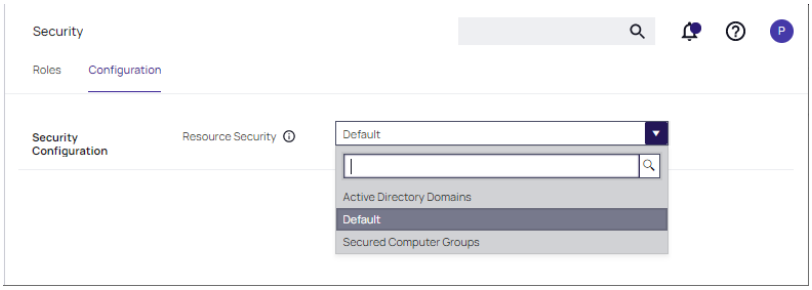
Select an existing role on the Roles page. The Role details page displays, where you can:

- Edit **Basic Details**.
- Click **x** to remove a user/resource or click **Add** to reselect resources.
- Select **Delete** at the **More** pull-down to delete the role.
- Select **Export** at the **More** pull-down to download a ZIP file of the role and children.



Security Configuration Tab

On the Configuration tab, Privilege ManagerAdmins specify the **Resource Security**. The Resource Security selection controls who can view data associated with specific computers.



- The **Default** option allows all Administrators, Users, and Helpdesk Users of Privilege Managerto have access.
- The **Secured Computer Groups** option allows for easier customization of which Roles have access to specific computers.
- The **Active Directory Domains** option allows customization of which Roles have access to associated AD Domain resources.

Application Roles

The following table provides an overview of Privilege Manager Application Roles.

Note: In general, the Privilege ManagerUser role can view reports, but access may be dependent on each report and the viewing rights assigned to the user's account.

Role	Summary	CRUD Users/Groups	View Reports	Run Tasks	Approve Approval Requests	Disclose Passwords	Modify Config, View Install Codes	Modify Policies, Filters, and LSS	View All Items	Upload Files	Create or Revoke Install Codes
Privilege Manager Administrators	Can do anything.	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes

Role	Summary	CRUD Users/Groups	View Reports	Run Tasks	Approve Approval Requests	Disclose Passwords	Modify Config, View Install Codes	Modify Policies, Filters, and LSS	View All Items	Upload Files	Create or Revoke Install Codes
Privilege Manager Field Engineering	Cannot do anything out of the box. Reserved for future use.										
Privilege Manager Helpdesk Users	This role has the least permissions. It can disclose passwords and manage approvals only.				yes	yes					
Privilege Manager macOS Administrators	Can do anything an administrator can, but only for macOS policies and resource targets.	yes (macOS)	yes	yes	yes	yes	yes	yes (macOS)	yes	yes	yes

Role	Summary	CRUD Users/Groups	View Reports	Run Tasks	Approve Approval Requests	Disclose Passwords	Modify Config, View Install Codes	Modify Policies, Filters, and LSS	View All Items	Upload Files	Create or Revoke Install Codes
Privilege Manager Unix/Linux Administrators	Can do anything an administrator can, but only for Unix/Linux policies and resource targets.	yes (Unix/Linux)	yes	yes	yes	yes	yes	yes (Unix/Linux)	yes	yes	yes
Privilege Manager Users	This is a read only role that can view all items, disclose passwords, and manage approvals.		yes		yes	yes			yes		

Role	Summary	CRUD Users/Groups	View Reports	Run Tasks	Approve Approval Requests	Disclose Passwords	Modify Config, View Install Codes	Modify Policies, Filters, and LSS	View All Items	Upload Files	Create or Revoke Install Codes
Privilege Manager View Password Role	Can only view current passwords and password change histories of managed users					yes					
Privilege Manager Windows Administrators	Can do anything an administrator can, but only for Windows policies and resource targets.	yes (Win)	yes	yes	yes	yes	yes	yes (Win)	yes	yes	yes

Setup

Refer to the Upgrade to learn more about Privilege Manager's setup feature for updates.

Tasks

In Privilege Manager tasks are activities that can be run on demand or regularly scheduled. If they are regularly scheduled, the schedule triggers the execution of a task instance, which performs specific actions based on set parameters.

Remote Scheduled Client Command type tasks that are considered agent-side require policies to be applied on the agent endpoints, the ones that are considered server-side do not require policies to be executed.

Note: With Privilege Manager v11.2.0, UTC support on task schedules has been deprecated. Delinea recommends to disable UTC on any configured task schedules.

Tasks are set-up via **Admin | More** and then selecting the Tasks link. They are categorized as following:

- Client Tasks - Scheduled Jobs default policies
- Server Tasks
- HelpDesk Tasks
- Infrastructure Scheduled Activities

The following general task topics are available:

- "Agent Hardening 10.7.1 and up" on page 206
- Maintenance tasks details
- Other tasks to schedule
  - Emailing Reports
- Reset Licensing
- Tasks Launching Executables without User Context

Note: Upgrading to Privilege Manager v10.8 causes a task to run to merge computer groups and remove unused system computer groups. This primarily affects the Application Control policies that are using resource targets/computer groups named **All Windows Computers with Application Control Agent Installed**. With v10.8, those policies will use the **Windows Computers** computer group and macOS will use **macOS Computers**.

If you want to prevent this automatic merge, modify the XML of this item:

`PrivilegeManager/#/item/xml/b2e02684-d154-48ca-9987-12b1759df822`

Add on line 2 `<adc:Attributes>NoModify</adc:Attributes>`.

Tasks Launching Executables

When a task is used to launch executables, but the task does not have an associated user context, the appropriate user token cannot be assigned. This applies to systems with v10.7 and above agents.

Example Scenario

A scheduled task launches an executable, which requires elevation, for example running the performance monitor process. That task is then set to run with elevated permissions, however not as a specific user, but rather as a local user group. Such task used in a policy will cause the executable to fail, since a specific user token cannot be associated.

Workaround

If you don't have a user context to assign to a task for launching an executable, you can use a PowerShell script in combination with the task and policy.

1. Create a PowerShell script to launch the executable.
2. Set the task to launch powershell.exe.
3. Pass in the name of the script.
4. Set the your policy to target that script.

Maintenance

Privilege Manager has many tasks that can be run to ensure that the data in the database is up-to-date and to purge old or unwanted information. This section provides an overview of the maintenance tasks and other schedulable tasks in #[PRODUCTNAME}#.

Determining how often to schedule maintenance tasks depends on the associated items, like events, files, computers, etc. and their build up. These tasks have default **parameters** assigned but are not scheduled to run. Privilege Manager administrators should schedule these tasks based on their needs and system performance.

The primary maintenance tasks that will need to be scheduled to ensure Privilege Manager databases do not grow too excessively are the

- Purge Maintenance - Application Control Events and
- Purge Maintenance - Files Undiscovered tasks and,
- in pre-10.5 systems, the
  - Purge Maintenance - Completed File Upload Sessions and
  - Purge Maintenance - Incomplete File Upload Sessions tasks.

Maintenance Tasks

These maintenance tasks can be found at

- **Admin | Configuration | General (tab)** or
- **Admin | Tasks | Jobs** and
- **Tasks | Infrastructure Scheduled Activities | Maintenance Tasks**.

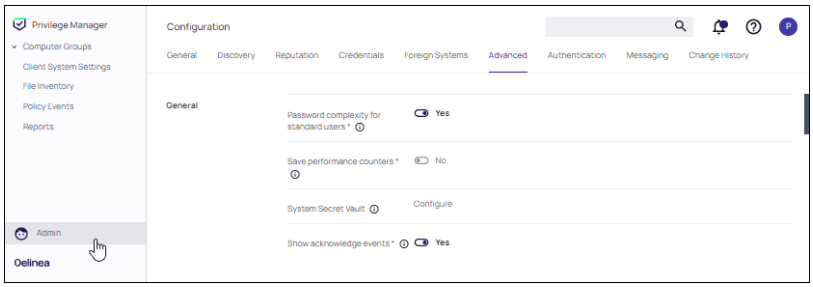
Assign Orphaned Agent Uploads

This task will assign agent event uploads that have been orphaned.

Parameters: Max records [default setting = 2500]

Delete Old Performance Counter Events

This task will delete internal Server performance counter events last updated before the specified time. You can check if performance counters are enabled by the **Save performance Counters** setting in **Admin** | **Configuration** (**Advanced** tab).



Parameters: Can be set to Seconds, Minutes, Hours, Days, and Weeks. The default is 1 Day.

This maintenance task should be used if Save Performance Counters is enabled in the general section of the advanced configuration settings.

Initialize Item Change History

This task is run after installs to ensure items with change tracking enabled have initial history entries. This is an automated task to populate initial states of items across updates.

LSS Migration Tasks

For information on the LSS Migration tasks refer to Migrate Local Security Policies.

Purge Agent and Gauge Data for Deleted Computers

This task will delete orphaned data from AgentActivity, AgentRegistration, and GaugeInstanceState.

> **Note:** This can be helpful to run, to remove unwanted data for computers that have been deleted from Privilege Manager.

Purge Duplicate Computers

Remove duplicate computers.

> **Note:** When AD sync occurs, Privilege Manager creates a new object in the database for each computer object. When the agent is installed, it references this same object. If the agent is installed before AD sync occurs, there can be 2 different objects in the database for the same machine. This task merges the duplicate objects and is usually only needed when agents are installed before a computer comes in from AD sync.

Purge Maintenance - Agent Logs

This server task will remove all Agent Log data that is older than the time period specified. This task is not enabled by default, since there is typically nothing in the logs to clear.

Parameters: Can be set to Seconds, Minutes, Hours, Days, and Weeks. The default is 1 Week.

Purge Maintenance - Application Control Events

Purges the selected Application Control Event types from the database using either of these methods:

- manually based on a specified range of time, or
- automatically after reaching a set threshold. Refer to Maximum Application Event Count time range specified.

This task is not enabled by default, so events remain until purged. We recommend using SysLog connector to send events for long term storage.

Note: If you are retaining data for 3-5 years, we recommend collecting a minimum amount of data since there is a maximum number of events enforced in the cloud. This is dependent on your licensing, but typically is 100,000 - 1,000,000 events.

Parameters: Event Types to Purge (Application Action Events, Application Justification Events, Application Metering Events, Application Verifier Events). All of these Application Control Events are populated in the various Application Action reports.

Note: Only Purge Events that belong to specific policies

Purge Application Control Events older than [default setting = 30 day(s)]

Note: Depending on policy settings, Application Control Events can pull a large amount of data into the database. Privilege Manager administrators must setup schedules for this task, as needed, to purge old or excessive data from Application Control policies.

Purge Maintenance - Audit Events

This task will remove audit event records older than the specified time period.

This task is not enabled by default, so events remain until purged. We recommend using SysLog connector to send events for long term storage.

Note: Audit Events are typically viewed via the **Change History** tab of the item in question.

Parameters: Purge events older than [default setting = 30 day(s)]

Note: The Audit events mainly pertain to and are used in Change History tracking. This task should not need to be scheduled.

Purge Maintenance - Completed File Upload Sessions

This task will remove completed file upload sessions older than the specified time period. This task becomes unnecessary since completed file uploads are purged automatically.

Parameters: Purge completed sessions older than [default setting = 1 day(s)]

Note: For versions 10.5 and later, the need to run this task should be significantly reduced since they are now cleaned up as file uploads complete.

Purge Maintenance - Files Undiscovered

Run this task to delete file resources which have not been discovered by File Inventory, and no agent can be identified to collect information for the files.

Parameters: Delete Files that have been undiscoverable for longer than [default setting = 1 week(s)]

Note: This task clears up files with the name "New Loaded Resource" that are older than X days. This can be a helpful task to schedule to remove undiscoverable files from the Event Discovery results (for example, temp files that an installer creates and then deletes).

Purge Maintenance - Incomplete File Upload Sessions

This task will remove incomplete file upload sessions older than the specified time period. This task is only used on as as-needed basis to clear incomplete items on a weekly or monthly basis.

Parameters: Purge incomplete sessions older than [default setting = 2 day(s)]

Note: For versions 10.5 and later, the need to run this task should be significantly reduced since they are now cleaned up as file uploads complete.

Purge Maintenance - Message History

This server task will remove all Message History data that is older than the time period specified. Message History data tracks all events received by the Privilege Manager Server and is used for informational purposes.

Parameters: Delete Message History older than [default setting = 30 day(s)]

Note: This task clears the `[Ams.Resource].[MessageHistory]` table. Use this task to purge that table, if it is excessively large.

Purge Maintenance - Excessively Correlated Change History

This task is no longer required.

Purge Maintenance - Orphaned Local Users and Groups

This task will delete local users and groups that reference a computer as their parent domain (which will block deletes), but are not part of that computers users and groups.

Purge Old Computers

Remove old computers and gauge data for old computers. Remove any agents that have not communicated with the server in a set number of days (default 90), resulting in a critical Agent state.

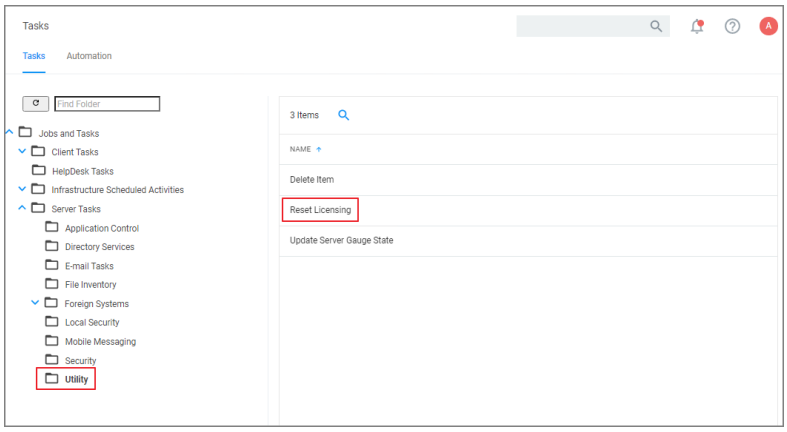
Reset Licensing

With Privilege Manager v10.7 and up license registrations can be reset. The Reset Licensing task allows upgrading users to remove outdated licenses.

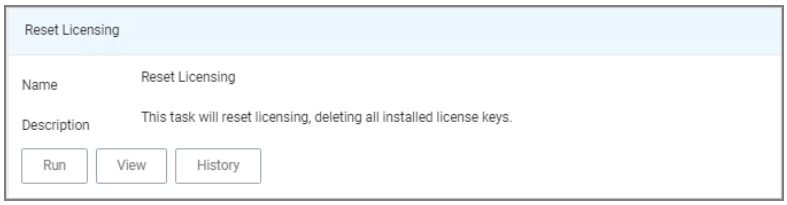
After acknowledging the license reset, all licenses are removed from the Privilege Manager instance. When no licenses can be found, the no product licenses warning banner displays on the top of the console.

Using the Reset Licensing Task

1. Navigate to the **Admin | Tasks**.
2. From the Tasks folder tree, select **Server Tasks | Utility**.
3. From the options on the right, select **Reset Licensing**.



Reset Licensing is a read-only task.



4. Click **Run**.

   To run the task, the user needs to acknowledge the removal of all installed license key.

   The task does not run without that acknowledgement and an error is generated.

   Note: Do not use the scheduling functionality on this task. After a license reset, new licenses should be applied ASAP.

To re-apply licenses refer to the information under Licensing in the Installation and Upgrades section.

Client Tasks

Client Tasks are used to run or schedule activities at the endpoints, like:

- Basic Inventory, which triggers the agent to immediately report basic inventory back to the server. The information can be viewed for a computer under Known Data. Data sets are different based on endpoint operating system.

- Resource Discovery Client Task, which populates agent-side data for any resources that have been discovered but lack detailed information.
- Update Applicable Policies, which triggers policy updates at the endpoints.

> **Note:** All default enabled client tasks **are read-only items** and if any customization to the schedule is required, create a copy to add, save, and apply changes. Schedule changes can be added on the Triggers page when clicking the existing schedule and then **Show Advanced**.

UTC support has been deprecated for these tasks. Delinea recommends to disable UTC on any configured task schedules.

These default or out-of-the-box client tasks are available via the **Scheduled Jobs** menu for each computer group. Details for each task are provided under the following topics:

- Basic Inventory
- Cleanup Agent Inventory Transfer
- COM Inventory Policy
- Cleanup Sent Privilege Manager Event
- Configure PM Remove Programs
- Default File Inventory Policy
- Deploy File Hash Exclusion Setting (Windows) - installed via Configuration Feeds only!
- Ensure UAC Override Setting
- Local User Inventory Policy
- Perform Resource Discovery
- Remove Successful Agent Events
- Reset ignored macOS software updates (macOS) - installed via Configuration Feeds only!
- Retry Errored TMS Events
- Set Agent Log Size
- Scheduled Check for Pending Tasks
- Shared Folder Inventory Policy
- Scheduled Registration
- Update Agent Commands
- Update Applicable Policies
- User Logon Inventory Policy
- Update Provisioned Resource Client Items
- Windows Service Inventory Policy

None Default Client Tasks

Client tasks can be created via **Admin | Tasks** on the Tasks tab by expanding **Jobs and Tasks** and selecting the **Client Tasks** folder.

Refer to Custom Client Tasks for examples and use cases.

Basic Inventory

Basic Inventory (Initial, Windows), (Initial, macOS), and (Initial, Unix/Linux) are scheduled to run at a client's initial start-up after the agent is installed. The cause of the policy's trigger is the task creation.

The common Basic Inventory is scheduled to run daily at a set time.

For Windows systems the policies instruct the agent on the client system to report the following WMI classes to the server:

- Win32_ComputerSystem,
- Win32_ComputerSystemProduct
- Win32_OperatingSystem WMI

Basic Inventory (Initial, Windows)

Parameter	Value
Default Active	Yes
Command	Perform WMI Basic Inventory (Windows)
Parameters	WMI classes: `ROOT\CIMV2:WIN32_ComputerSystemProduct`, `ROOT\CIMV2:Win32_ComputerSystem`, `ROOT\CIMV2:Win32_OperatingSystem`
Triggers	Daily at 10:00:00 AM
	Upon task creation/modification
Targets	All Windows Managed Computers - No Basic Inventory (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 5 minutes.
(retry on failure)	Not set by default

Parameter	Value
Rule	Default (Do not start a new instance)
Agent Sent Size	250 KB
Agent Received Size	n/a
Restrictions	None

Basic Inventory (Windows)

Parameter	Value
Default Active	Yes
Command	Perform WMI Basic Inventory (Windows)
Parameters	WMI classes: `ROOT\CIMV2:WIN32_ComputerSystemProduct`, `ROOT\CIMV2:Win32_ComputerSystem`, `ROOT\CIMV2:Win32_OperatingSystem`
Triggers	Daily at 8:00:00 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 5 minutes.
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	

Basic Inventory (Initial, macOS)

Parameter	Value
Default Active	Yes
Command	Perform Basic Inventory (macOS)
Triggers	Daily at 10:00:00 AM
	Upon task creation/modification
Targets	All macOS Managed Computers - No Basic Inventory (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 5 minutes.
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	

Basic Inventory (macOS)

Parameter	Value
Default Active	Yes
Command	Perform Basic Inventory (macOS)
Triggers	Daily at 10:00:00 AM
Targets	macOS Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand

Parameter	Value
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 5 minutes.
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	

Basic Inventory (Initial, Unix/Linux)

This scheduled task triggers Unix/Linux agents who have not already sent basic inventory to send it for the first time.

Note: Privilege Manager for Linux/Unix and Windows for servers is End of Sale/Renewal only.

Parameter	Value
Default Active	Yes
Command	Perform Basic Inventory (Unix/Linux)
Triggers	Daily at 10:00:00 AM
	Upon task creation/modification
Targets	Unix/Linux Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 5 minutes.
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	

Parameter	Value
Agent Received Size	
Restrictions	

Basic Inventory (Unix/Linux)

This scheduled task triggers Unix/Linux agents who have already sent initial basic inventory.

Parameter	Value
Default Active	Yes
Command	Perform Basic Inventory (Unix/Linux)
Triggers	Daily at 10:00:00 AM
	Upon task creation/modification
Targets	Unix/Linux Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 5 minutes.
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	

Cleanup Agent Inventory Transfer

Completes and cleans BITS transfers and temporary files used by the TMS Agent Inventory Helper.

Cleanup Agent Inventory Transfers (Windows)

Parameter	Value
Default Active	Yes
Command	Cleanup Agent Inventory Transfers
Triggers	Daily at 2:00:02 AM
Targets	10.8: Windows Computers
	Legacy: All Windows Computers with Application Control Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 30 minutes.
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on number of failed file transfers
Agent Received Size	n/a
Restrictions	None

COM Inventory Policy

The purpose of this policy is to inventory COM+ and DCOM packages installed on the client. The inventory of these package

COM+ (Component Object Model) and DCOM (Distributed Component Object Model) utilize RPC calls for component communication and access to the object's methods and data. Running an inventory on those packages on a client is beneficial, if apps using those packages require elevation or should be denied.

Parameter	Value
Default Active	No
Command	Local Security COM Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM

Parameter	Value
	Upon task creation/modification
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s) - not set by default.
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on number of COM+ and DCOM packages
Agent Received Size	n/a
Restrictions	None

Cleanup Sent Privilege Manager Events

Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.

Cleanup sent Privilege Manager Events (Windows)

Parameter	Value
Default Active	Yes
Command	Remove sent TMS Client Events (Windows)
Triggers	Daily at 2:00:02 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 30 minutes.

Parameter	Value
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	None

Cleanup sent Privilege Manager Events (macOS)

Parameter	Value
Default Active	Yes
Command	Remove sent TMS Client Events (macOS)
Triggers	Daily at 2:30:02 AM
Targets	macOS Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 30 minutes.
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	None

Configure Privilege Manager Remove Programs

Configure the Privilege Manager Remove Programs behavior.

For standard users the utility by default,

- adds all programs to the Control Panel.
- hides repair options for all installers.
- shows the blocked installer list.
- prevents Delinea software from being uninstalled.

Parameter	Value
Default Active	Yes
Command	Configure Remove Programs Application
Parameters	selected: Add to Control Panel, Hide Repair for All Installers, Show Blocked Installers in List, Vendor software that can't be Uninstalled: Thycotic.
Triggers	Daily at 10:00:00 PM (repeating every 2 hours for a duration of 24 hours)
	Upon task creation/modification
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 3 day(s).
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	None

Default File Inventory Policy

The purpose of this policy is to inventory software programs running on the managed computer.

These policies use their respective OS based File Specification filters, which in turn have a set of optional additional filters to identify the programs to be inventoried.

Default File Inventory Policy (Windows)

Parameter	Value
Default Active	Yes
Command	File Inventory Command
Parameters	Default File Specification (Windows)
Triggers	Weekly on Sun at 3:00:00 AM
Targets	All Windows Computers with File Inventory Agent Installed (Target)
Conditions	Idle: None specified by default
	Power: Start the task only if the computer is on AC power, Stop if the computer switches to battery power
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 3 day(s).
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on number of programs to inventory
Agent Received Size	n/a
Restrictions	None

Default File Inventory Policy (macOS)

Parameter	Value
Default Active	Yes
Command	File Inventory Command
Parameters	Default File Specification (macOS), Default App Bundles File Specification Filter
Triggers	Weekly on Sun at 3:00:00 AM

Parameter	Value
Targets	All macOS Computers with File Inventory Agent Installed (Target)
Conditions	Idle: None specified by default
	Power: Start the task only if the computer is on AC power, Stop if the computer switches to battery power
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 3 day(s).
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on number of programs to inventory
Agent Received Size	n/a
Restrictions	None

Ensure UAC Override Setting (Windows)

Ensures that the UAC Override Registry Key is set.

Parameter	Value
Default Active	Yes
Command	Ensure UAC Override Registry Key
Parameters	Default File Specification (Windows)
Triggers	Daily at 12:00:00 AM
	At startup
Targets	10.8: Windows Computers
	Legacy: All Windows Computers with Application Control Agent Installed (Target)
Conditions	None specified by default

Parameter	Value
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 15 minute(s).
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	None

Exclude File Extensions during File Hashing

The Delinea Application Control Agent collects the file hash of a new process and also the hashes of the child processes it runs. Sometimes non-executable file types cause execution issues during the hashing process. Via the downloadable Configuration Feeds, Delinea offers a policy template that provides the ability to exclude certain file extensions from the hash process.

If non-executable files like xlsx, xls, mdb, and accdb for example cause execution issues, download the **Secondary Hash Exclusions** policy template. By default .mdb and .accdb are excluded from the file hashing procedure in Privilege Manager. To not overwrite default behavior, make them a part of your exclude list at all times.

Always manually test a new policy deployment on a single endpoint, and only push the solution to all desired workstations after a successful verification on the test environment.

Note: This feature requires a Delinea Control Agent version of 10.5 or greater and is **only available via Configuration Feeds installation**.

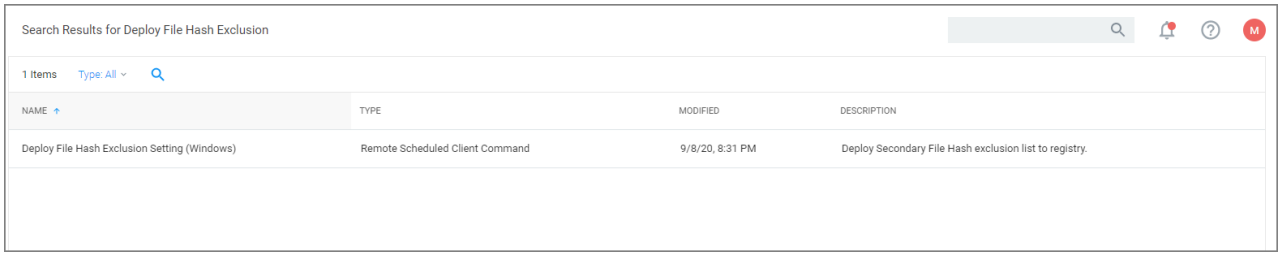
Default File Inventory Policy (Windows)

Parameter	Value
Default Active	No
Command	Deploy Secondary Hash Exclusions Registry Key
Parameters	Comma-separated List of extensions to exclude, default: *mdb,accdb*
Triggers	Default: Daily at 10:00:00 PM starting Tue Jul 31 2018 (repeating every 2 hours for a duration of 24 hours)
	Default: Upon task creation/modification

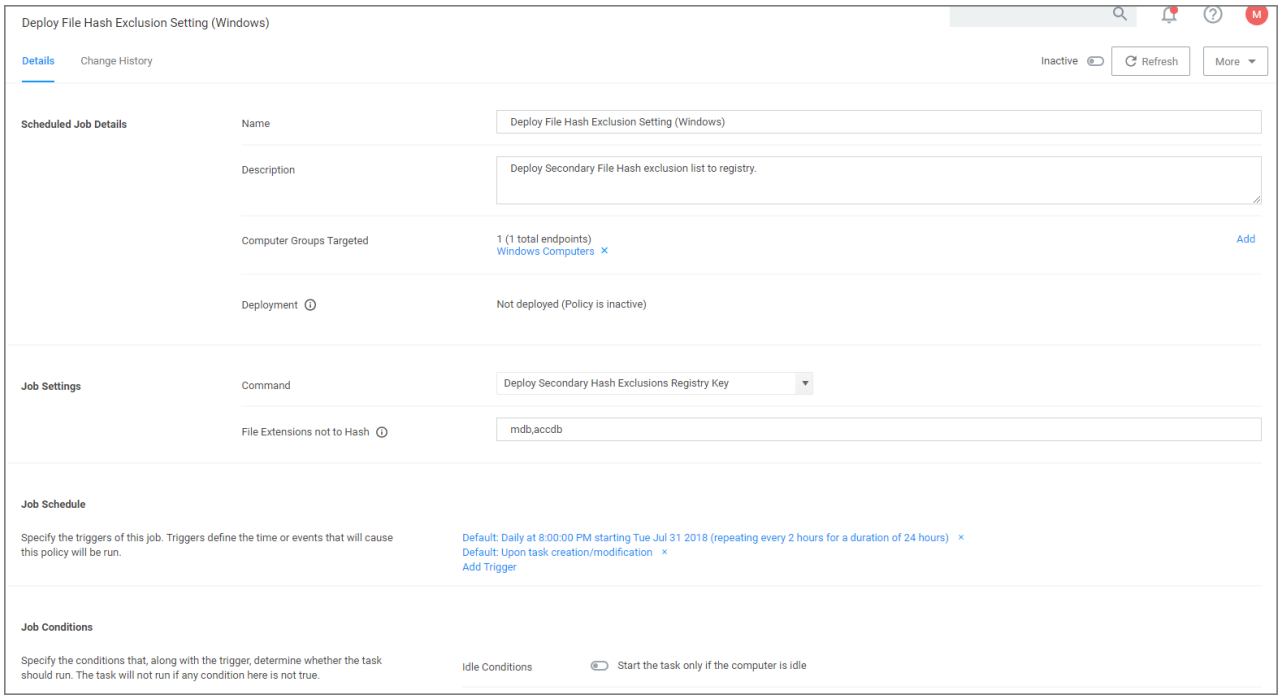
Parameter	Value
Targets	Windows Computers
Conditions	Idle: None specified by default
	Power: Start the task only if the computer is on AC power, Stop if the computer switches to battery power
Advanced	On: Allow task to be run on demand
	Off: Run task as soon as possible after a scheduled start is missed
	Off: Stop the task if it run for longer than 3 day(s).
	Off: If the task fails, attempt to restart
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	None

Create File Exclusion through Config Feed

1. Navigate to **Admin | Config Feeds** link.
2. Expand **Privilege Manager Configuration Feeds**.
3. Expand **Application Control Solution**.
4. Locate the **Application Control - Secondary Hash Exclusions** and click **Install**. The policy template is being downloaded and installed.
5. After the successful installation of the configuration feed, use **Search** and type **Secondary Hash Exclusion**.
6. From the results list select the new policy **Deploy File Hash Exclusion Setting (Windows)**.



7. Under **Job Settings | File Extensions not to Hash** you can add to the list of extensions, for example xlsx, xls. By default *.mdb* and *.accdb* extensions are already listed.



8. Click **Save Changes**.

Manually Test on Workstation

To create manual secondary extension exceptions to file hash collection, add a registry key to the workstation.

1. Open Registry Editor (regedit.exe) and navigate to

   `HKLM:\Software\Policies\Arellia\AMS.`

2. Create **New | String Value**
   a. Name: **SecondaryExtensionExclusions**
   b. Value: enter a comma-separated list of extensions to include, i.e. `xlsx,xls,mdb,accdb`.
3. Restart the Thycotic services on this machine.

Open a file matching an extension from your inclusion list and test if it works on this workstation. If it works, create a Policy to push this registry key creation to all desired workstations.

Local User Inventory Policy

The purpose of this policy is to inventory Local User accounts, groups and group membership on the client. This policy can also be used to inventory specific account privileges.

Local User Inventory Policy

Parameter	Value
Default Active	Yes
Command	Local Security Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM
	Upon task creation/modification
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s) - not set by default.
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on the number of users and groups
Agent Received Size	n/a
Restrictions	GPO - Audit Account Management enabled does not use Security Event Log

Local User Inventory Policy (macOS)

Parameter	Value
Default Active	Yes
Command	Local Security Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM
	Upon task creation/modification
Targets	macOS Computers
Conditions	None specified by default

Parameter	Value
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s) - not set by default.
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on the number of users and groups
Agent Received Size	n/a
Restrictions	None

Perform Resource Discovery

Schedule on which agents check with server to determine, if any local resources require discovery.

After any type of resource discovery, it might be possible that the server does not have all the details required to correctly identify what was initially provided by the agent. The agent periodically checks in with the server, if any additional information needs to be discovered. The server then sends information back to the agent about any pending item clarifications.

Perform Resource Discovery (Windows)

Parameter	Value
Default Active	Yes
Command	Resource Discovery Command
Triggers	Daily at 12:00:00 AM (repeating every 4 hours for a duration of 24 hours)
	Upon task creation/modification
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 1 hour.

Parameter	Value
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on server request
Agent Received Size	Depends on request volume and the number of items pending on server for clarification
Restrictions	None

Perform Resource Discovery (macOS)

Parameter	Value
Default Active	Yes
Command	Resource Discovery Command
Triggers	Daily at 3:00:00 AM (repeating every 4 hours for a duration of 24 hours)
	Upon task creation/modification
Targets	macOS Computers
Conditions	Idle: None specified by default
	Power: Start the task only if the computer is on AC power, Stop if the computer switches to battery power
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 3 day(s).
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on server request
Agent Received Size	Depends on request volume and the number of items pending on server for clarification
Restrictions	None

Retry Errored TMS Events

Scan Agent queue for any events that require retransmission.

Retry errored TMS Events (Windows)

Parameter	Value
Default Active	Yes
Command	Retry errored TMS Client Events (Windows)
Parameters	Force Resending (incl. transient errors)
Triggers	Daily at 2:00:02 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 1 hour(s).
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on number of items that require retransmission
Agent Received Size	n/a
Restrictions	None

Retry errored TMS Events (macOS)

Parameter	Value
Default Active	Yes
Command	Retry errored TMS Client Events (macOS)
Triggers	Daily at 2:00:02 AM
Targets	macOS Computers

Parameter	Value
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 1 hour(s).
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on number of items that require retransmission
Agent Received Size	n/a
Restrictions	None

Remove Successful Agent Events

Remove Successful Agent Events (Unix/Linux)

This command will remove agent events that have been successfully uploaded to Privilege Manager.

Parameter	Value
Default Active	Yes
Command	Remove Successful Agent Events (Unix/Linux)
Triggers	Daily at 2:30:02 AM
Targets	Unix/Linux Computers
Deployment	
Conditions	None specified by default
Advanced	On: Allow task to be run on demand
	On: Run task as soon as possible after a scheduled start is missed
	Off: If the task fails, attempt to restart
	On: Stop the task if it runs for longer than 5 minute(s).

Parameter	Value
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	None

Set Agent Log Size

Configures the size of the Agent Event Log. By default this is set to 1 MB. For most environments it is recommended to increase the Agent Event Log size. This task can be used to override the default setting.

Parameter	Value
Default Active	No
Command	Set Agent Log Size (Windows)
Parameters	Log Size: 20 MB
Triggers	Daily at 6:00:00 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	None

Scheduled Check for Pending Tasks

Scheduled Check Pending Client Tasks - Internet Clients (Windows)

Initiate a check for pending client tasks. Used by agents that are unable to receive an incoming connection from the server.

Parameter	Value
Default Active	Yes
Command	Check Pending TMS Client Tasks
Triggers	Daily at 2:00:00 AM (repeating every 4 hours)
Targets	All Windows Managed Computers - Internet Client (Target)
Conditions	None specified by default
Advanced	On: Allow task to be run on demand
	On: Run task as soon as possible after a scheduled start is missed
	Off: If the task fails, attempt to restart
	On: Stop the task if it runs for longer than 5 minute(s).
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	Depends on number of pending items
Restrictions	None

Shared Folder Iventory Policy

The purpose of this policy is to inventory shared folders on the client.

Parameter	Value
Default Active	No
Command	Local Security Shared Folder Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM
Targets	All Windows Computers with Local Security Agent Installed (Target)

Parameter	Value
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on number of shared folders on the endpoint
Agent Received Size	n/a
Restrictions	None

Scheduled Registration

Scheduled Registration (Windows)

Initiate agent registration with server.

Parameter	Value
Default Active	Yes
Command	Check Pending TMS Client Tasks
Triggers	Daily at 2:00:00 AM (repeating every 4 hours)
Targets	All Windows Managed Computers - Internal Network (Target)
Conditions	None specified by default
Advanced	On: Allow task to be run on demand
	On: Run task as soon as possible after a scheduled start is missed
	Off: If the task fails, attempt to restart
	On: Stop the task if it runs for longer than 5 minute(s).
Rule	Default (Do not start a new instance)

Parameter	Value
Agent Sent Size	5 KB
Agent Received Size	n/a
Restrictions	None

Scheduled Registration - Internet Clients (Windows)

Initiate agent registration with server less frequently than internal clients.

Parameter	Value
Default Active	Yes
Command	Check Pending TMS Client Tasks
Triggers	Daily at 2:00:00 AM (repeating every 4 hours)
Targets	All Windows Managed Computers - Internet Client (Target)
Conditions	None specified by default
Advanced	On: Allow task to be run on demand
	On: Run task as soon as possible after a scheduled start is missed
	Off: If the task fails, attempt to restart
	On: Stop the task if it runs for longer than 5 minute(s).
Rule	Default (Do not start a new instance)
Agent Sent Size	5 KB
Agent Received Size	n/a
Restrictions	None

Scheduled Registration (macOS)

When this policy is triggered the Agent will attempt (or re-attempt) to register with the server.

Parameter	Value
Default Active	Yes

Parameter	Value
Command	Start TMS Registration
Triggers	Daily at 2:00:00 AM (repeating every 1 hour for a duration of 24 hours)
Targets	All macOS Managed Computers - Internal Network (Target)
Conditions	None specified by default
Advanced	On: Allow task to be run on demand
	On: Run task as soon as possible after a scheduled start is missed
	Off: If the task fails, attempt to restart
	On: Stop the task if it runs for longer than 5 minute(s).
Rule	Default (Do not start a new instance)
Agent Sent Size	5 KB
Agent Received Size	n/a
Restrictions	None

Scheduled Registration (Unix/Linux)

This agent-scheduled task refreshes registration data for the assigned agents.

Parameter	Value
Default Active	Yes
Command	Start TMS Registration
Triggers	Daily at 2:00:00 AM (repeating every 1 hour for a duration of 24 hours)
Targets	Unix/Linux Computers
Deployment	
Conditions	None specified by default
Advanced	On: Allow task to be run on demand
	On: Run task as soon as possible after a scheduled start is missed

Parameter	Value
	Off: If the task fails, attempt to restart
	On: Stop the task if it runs for longer than 5 minute(s).
Rule	Default (Do not start a new instance)
Agent Sent Size	5 KB
Agent Received Size	n/a
Restrictions	None

Update Agent Commands

Task sends up request for hashes of specific client item types. With Privilege Manager version 10.7 and up returned items are filters based on the last time run the task ran.

Update Agent Commands (Windows)

Instructs Agent to update any agent commands if required.

Parameter	Value
Default Active	Yes
Command	Force Client Item Update Command
Parameters	Category: Agent Command
Triggers	Daily at 12:00:00 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 10 minute(s).
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	

Parameter	Value
Agent Received Size	
Restrictions	None

Update Agent Commands (macOS)

When this policy is triggered the Agent will update agent command items.

Parameter	Value
Default Active	Yes
Command	Force Client Item Update Command
Parameters	Category: Agent Command
Triggers	Daily at 12:00:00 AM
Targets	macOS Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 10 minute(s).
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	Depends on the number of updated commands
Restrictions	None

Update Applicable Policies

Update Applicable Policies (Windows)

Instructs Agent to check with server for policy changes.

Parameter	Value
Default Active	Yes
Command	Update Applicable Policies
Triggers	Daily at 12:00:00 AM (repeating every 30 minutes for a duration of 24 hours)
Targets	All Windows Managed Computers - Internal Network (Target)
Conditions	None specified by default
Advanced	On: Allow task to be run on demand
	On: Run task as soon as possible after a scheduled start is missed
	Off: If the task fails, attempt to restart
	On: Stop the task if it runs for longer than 5 minute(s).
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	None

Update Applicable Policies - Internet Clients (Windows)

Instructs Agent to check with server for policy changes less frequently than internal clients.

Parameter	Value
Default Active	Yes
Command	Update Applicable Policies
Triggers	Daily at 12:00:00 AM (repeating every 2 hours for a duration of 24 hours)
Targets	All Windows Managed Computers - Internet Client (Target)
Conditions	None specified by default
Advanced	On: Allow task to be run on demand
	On: Run task as soon as possible after a scheduled start is missed

Parameter	Value
	Off: If the task fails, attempt to restart
	On: Stop the task if it runs for longer than 5 minute(s).
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	None

Update Applicable Policies (macOS)

When this policy is triggered the Agent will check the server for updated policies.

Parameter	Value
Default Active	Yes
Command	Update Applicable Policies
Triggers	Daily at 12:00:00 AM (repeating every 30 minutes for a duration of 24 hours)
Targets	All macOS Managed Computers - Internal Network (Target)
Conditions	None specified by default
Advanced	On: Allow task to be run on demand
	On: Run task as soon as possible after a scheduled start is missed
	Off: If the task fails, attempt to restart
	On: Stop the task if it runs for longer than 5 minute(s).
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	Depends on the number of updated policies
Restrictions	None

Update Applicable Policies (Unix/Linux)

This remote-scheduled command will update policies applicable to the assigned agents.

Parameter	Value
Default Active	Yes
Command	Update Applicable Policies
Triggers	Daily at 12:00:00 AM (repeating every 2 hours for a duration of 24 hours)
Targets	Unix/Linux Computers
Deployment	
Conditions	None specified by default
Advanced	On: Allow task to be run on demand
	On: Run task as soon as possible after a scheduled start is missed
	Off: If the task fails, attempt to restart
	On: Stop the task if it runs for longer than 5 minute(s).
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	None

User Logon Inventory Policy

Updates user logon data based on a given schedule to provide primary user information.

Parameter	Value
Default Active	Yes
Command	Windows Logon Event Processor
Triggers	Weekly on Sun at 2:00:00 AM
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand

Parameter	Value
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on number of user sessions
Agent Received Size	n/a
Restrictions	None

Update Provisioned Resource Client Items

These policies trigger the Agent to force a Client Item Update for provisioned resources on the specific client system.

Update Provisioned Resource Client Items (Windows)

Parameter	Value
Default Active	Yes
Command	Force Client Item Update Command
Parameters	Category: Provisioned Resource
Triggers	Daily at 8:00:00 AM starting Sun Apr 07 2013
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on the number of provisioned items

Parameter	Value
Agent Received Size	n/a
Restrictions	None

Update Provisioned Resource Client Items (macOS)

Parameter	Value
Default Active	Yes
Command	Force Client Item Update Command
Parameters	Category: Provisioned Resource
Triggers	Daily at 8:00:00 AM starting Sun Apr 07 2013
Targets	All macOS Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on the number of provisioned items
Agent Received Size	n/a
Restrictions	None

Windows Service Inventory Policy

The purpose of this policy is to inventory Windows Services on the client.

Parameter	Value
Default Active	Yes
Command	Local Security Service Inventory Command

Parameter	Value
Triggers	Weekly on Sun at 2:00:00 AM
	Upon task creation/modification
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it ran for longer than 0 minute(s). - not set by default
(retry on failure)	Not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	Depends on the number of installed windows services
Agent Received Size	n/a
Restrictions	None

Custom Client Tasks

Custom client tasks can be created on the following folder levels:

- Client Tasks
  - Client Item Updates
  - Directory Services
  - Event Maintenance
  - File Inventory
  - Local Security

Refer to these examples:

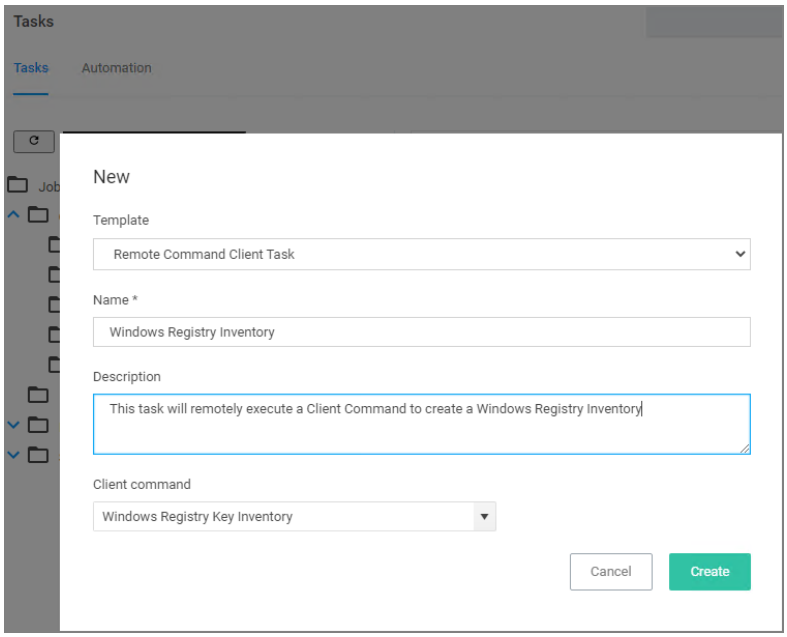
- Windows Registry Inventory

Windows Registry Inventory

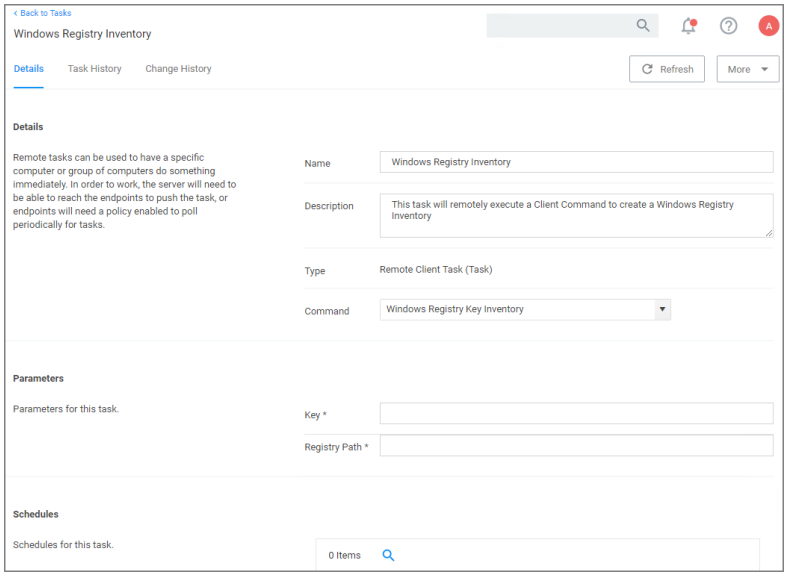
The Windows Registry Inventory task executes a client command to create a Windows Registry Inventory.

1. Navigate to **Admin | Tasks**.
2. On the **Tasks** tab under **Jobs and Tasks**, click on **Client Tasks**.

3. Click **Create**.
4. From the **Template** drop-down, select **Remote Client Task**.
5. From the **Client command** drop-down, select **Windows Registry Inventory**.
6. Copy the command name to paste it into the Name field or enter a name to reflect your use case.
7. Modify the description.



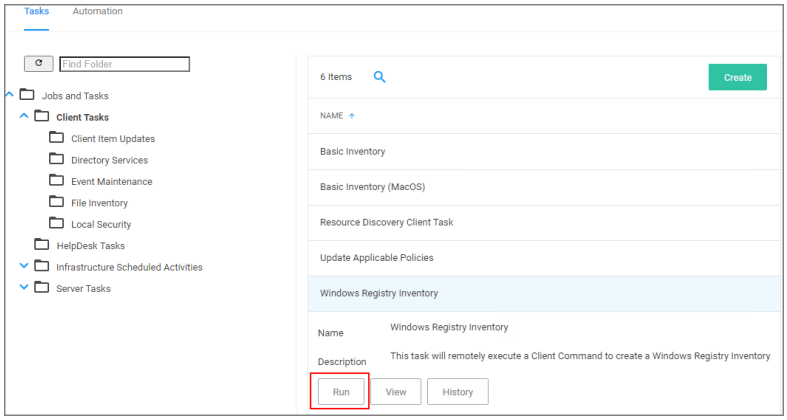
8. Click **Create**.



Customizing the Windows Registry Inventory Task

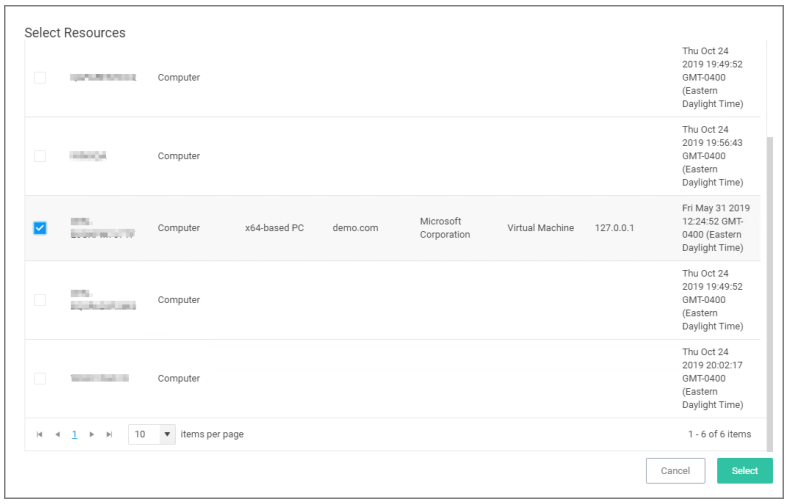
To be able to run the task, the key and registry path information needs to be provided. There are two options to run the task, via:

- the Windows Registry Inventory page or
- Run Task under the task quick view list:



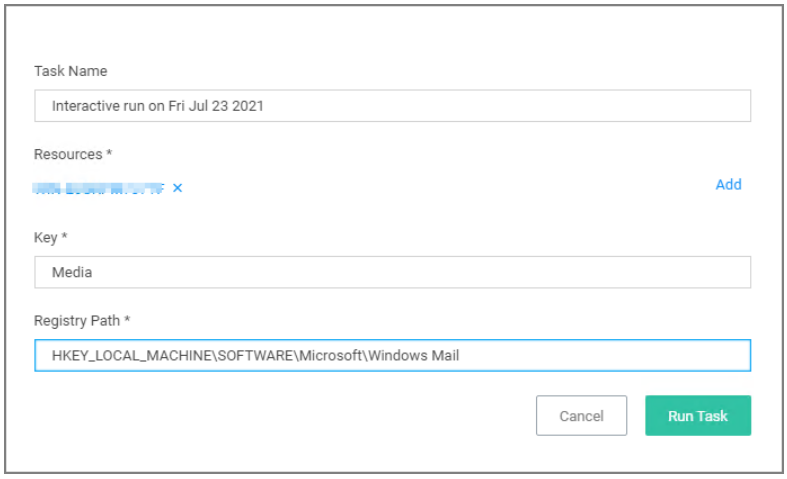
Using the Windows Registry Inventory page

1. On the Windows Registry Inventory task page under Parameters, enter the **Key** information, e.g. `Media`.
2. Enter the Registry Path, e.g. `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Mail`.
3. Click **Save Changes**.
4. From the **More** drop-down, select **Run Task**.
5. Add any number of resources you want to target with this task.



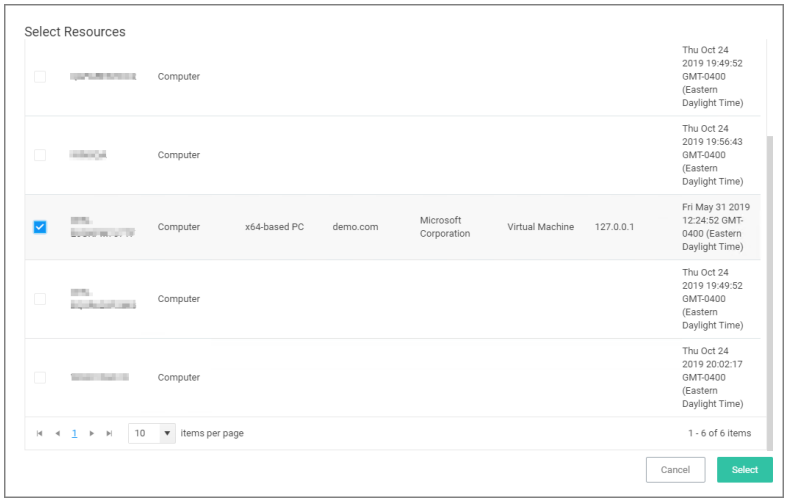
Note: Do not run this task for macOS or Unix/Linux agent endpoints, only select agent endpoints on Windows systems.

6. Click **Run Task**.



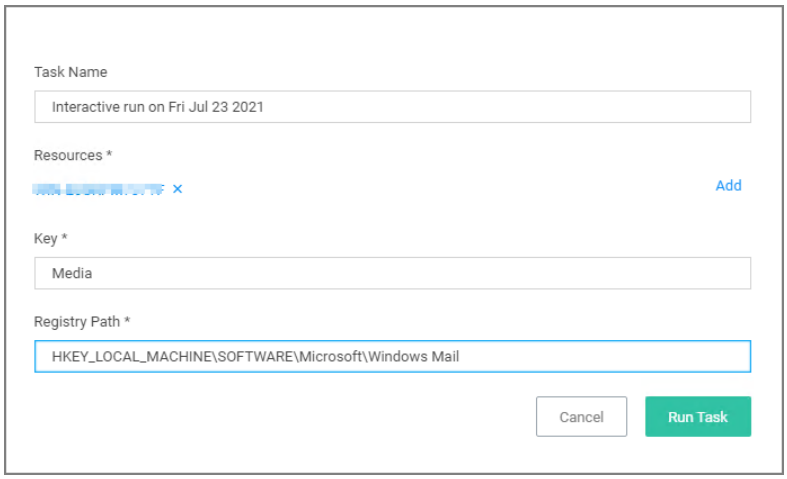
Using the Quick View List Options

1. Select your Windows Registry Inventory task from the task list.
2. Click **Run**.
3. Add any number of resources you want to target with this task.



Note: Do not run this task for macOS or Unix/Linux agent endpoints, only select agent endpoints on Windows systems.

4. Enter the Key value.
5. Enter the Registry Path value.

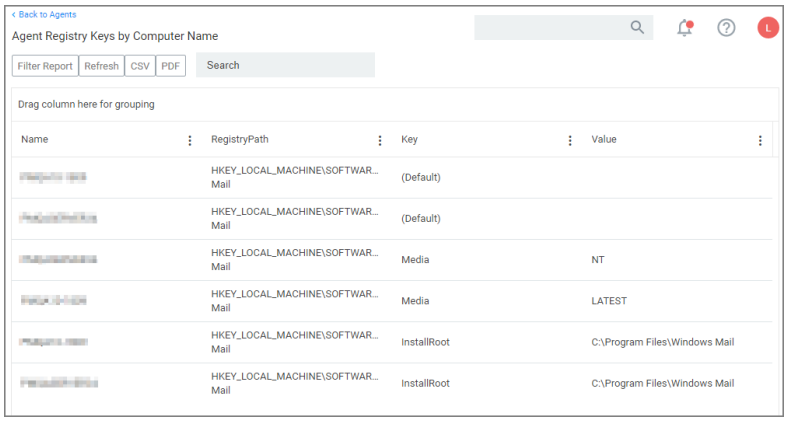


6. Click **Run Task**.

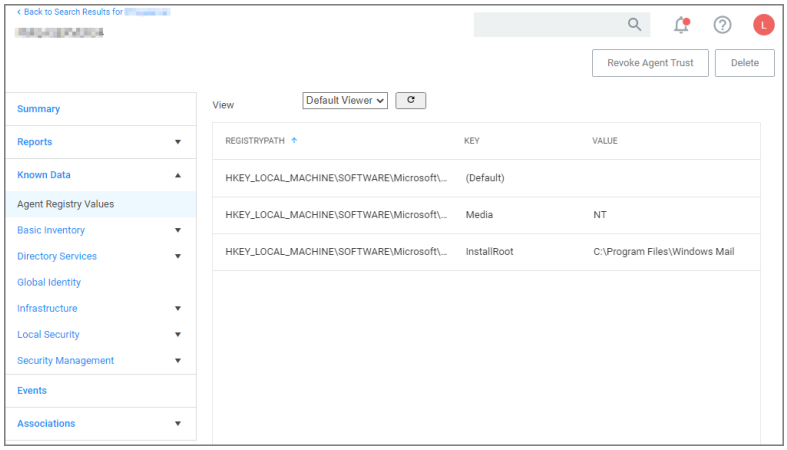
View the Results

The results of the task execution can be viewed via either Agent Reports or Known Data in the Resource Explorer:

- Navigate to **Admin | Agents | Agent Reports (tab) | Agent Registry Keys By Computer Name**:



- Navigate to the Computer Resource page and select **Known Data | Agent Registry Values**:



Helpdesk Tasks

By default this folder is empty. Administrators can use it to copy tasks for HelpDesk users to run them. The HelpDesk folder provides security settings on those folders that would grant permissions if someone puts tasks in that area.

Infrastructure Scheduled Activities

These are tasks that pertain to either core functions or to components and subcomponents of Privilege Manager.

Component	Task	Description
Core, no folder at root level	Client Items Update **OBSOLETE WITH v10.7 and higher**	Updates client items required by agents.
	Collection and Resource Targeting Update	Updates collections and resource targets.
	Collection Update	Update collections.
	Import Local Group Policy Definitions	Loads Group Policy Definitions from the local machine.

Component	Task	Description
	Import Secret Server Licenses	A scheduled import of licenses from Secret Server.
	Licensing Update	Updates licensing product counts.
	Resource Discovery	Run this task to populate data for resources that have been discovered but lack detailed information.
	Resource Target Update	Use this task to updates resource targeting.
Application Control		
App Control Cylance	Refresh Cylance Security Rating Report	Refreshes Cylance security rating reports on a schedule.
App Control VirusTotal	Recalculate Ratings for VirusTotal Provider	Recalculates security rating levels for resource rated by the given provider.
	Refresh VirusTotal Security Rating Reports	Refreshes VirusTotal security rating reports on a schedule.
Approval	ServiceNow Approval	Initiates a ServiceNow approval process and waits for the result.
Configuration	Reconfigure for System Secret Vault Change	This task is run by the system when the configured system secret vault setting has changed.
Data Feed	Content Tasks	Download Data Feed Entry - Download Data Feed Entity.
		Import Data Feed Entry - Imports data feed entities and their corresponding data feeds, primarily designed to be used by the Setup component.
		Import Product Configuration Package - Download Data Feed Entity.

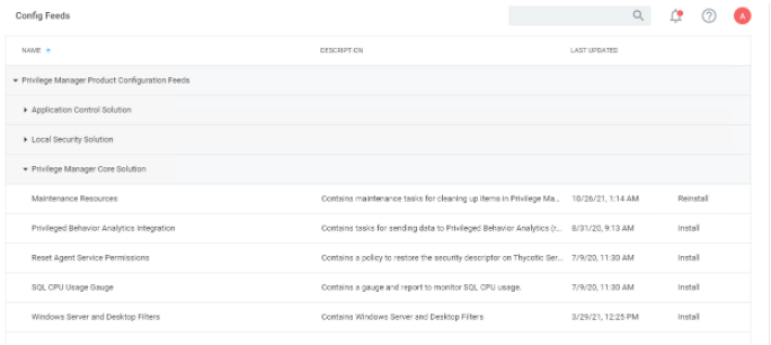
Component	Task	Description
	Update Tasks	Clear Data Feed Entity Updated - Clear Data Feed Entity.
		Update Data Feed - Updates the Privilege Manager Configuration Feed List
		Update TMS Configuration List Data Feed - Updates the Privilege Manager Configuration Feed List.
Directory Services	Active Directory Merge Computers	Merges computers created by Directory Services.
	Active Directory Merge Single Computer	Merges a single computer during agent registration. Needed if AD Sync has occurred before agent registration.
	Import Secret Server Domains	A scheduled import of AD domains from Secret Server.
	OU Directory Scope Collection Update	This task updates the membership of Directory Services OU scope collections.
	Promote Windows Domains	Promotes any Windows domains to Active Directory domains.
	Update Active Directory Details	Updates Active directory domain details including domain controllers.
File Inventory	Update File Filter Security Catalogs	Updates security catalogs associated with File Collection Security Catalog Filter items.
Import Activities	Import Packages	Imports multiple product packages, data feed entries and performs initial configuration, primarily designed to be used by the Setup component.
	Import Packages v3	Imports multiple product packages, data feed entries and performs initial configuration, primarily designed to be used by the Setup component.
	Install Products V4	This task installs product NuGet packages.

Component	Task	Description
	Install Products V4 (Server Nodes)	This task is used to upgrade binaries for additional server nodes.
	Install Products V5	This task installs product NuGet packages.
	Install Products V5 (Server Nodes)	This task is used to upgrade binaries for additional server nodes.
Local Security	Primary User Update	Updates the primary user for each computer in the given collection.
	User Credentials Data Update	This task ensures that resource credentials match the source user data.
Maintenance Tasks	Assign Orphaned Agent Uploads	This task assigns agent event uploads that have been orphaned.
	Delete Old Performance Counter Events	This task deletes internal performance counter events last updated before the specified time.
	Purge Maintenance - Agent Logs	This server task removes all Agent Log data that is older than the time period specified.
	Purge Maintenance - Application Control Events	Purges the selected Application Control Event types from the database based on the time range specified.
	Purge Maintenance - Audit Events	This task removes audit event records older than the specified time period.
	Purge Maintenance - Completed File Upload Sessions	This task removes completed file upload sessions older than the specified time period.

Component	Task	Description
	Purge Maintenance - Files Undiscovered	Run this task to delete file resources which have not been discovered by File Inventory, and no agent can be identified to collect information for the files.
	Purge Maintenance - Incomplete File Upload Sessions	This task removes incomplete file upload sessions older than the specified time period.
	Purge Maintenance - Message History	This server task removes all Message History data that is older than the number of seconds/minutes/hours/days/weeks specified. Message History data tracks all events received by the Privilege Manager Server and is used for information purposes.
	Purge Old Computers	Removes old computers and gauge data for those old computers.
	Purge Old Unmanaged AD Computers	Deletes unmanaged computers, imported from Active Directory, that have not been updated in 90 days by default.
Monitoring	Check for Available Product Updates	Checks the configured `nuget:source:SolutionCentre` for available product updates.

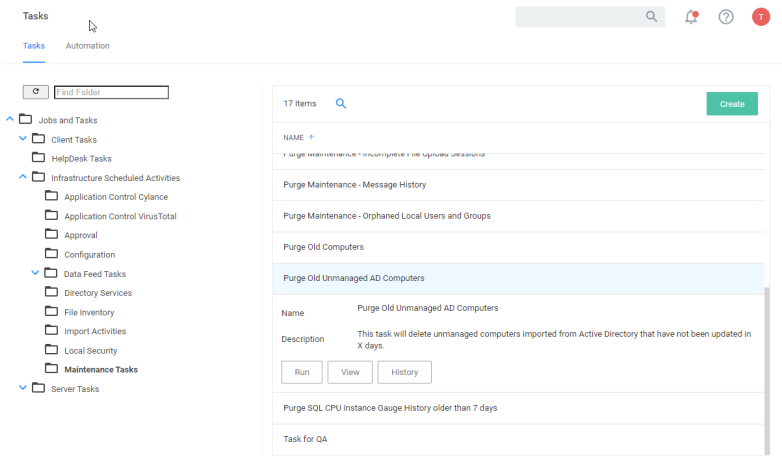
Purge Old Unmanaged AD Computers

1. Navigate to **Admin | Config Feeds**.
2. Install the **Maintenance Resource**, located under **Privilege Manager Product Configuration Feeds | Privilege Manager Core Solution**.



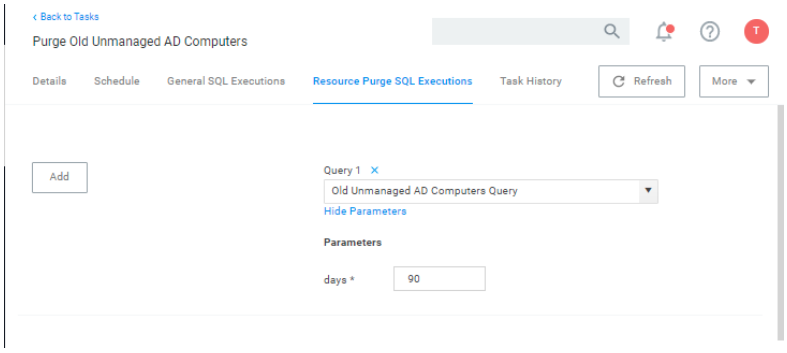
3. Navigate to **Admin | Tasks | Jobs and Tasks | Infrastructure Scheduled Activities | Maintenance Tasks**, select **Purge Old Unmanaged AD Computers**.

   This task deletes unmanaged computers, imported from Active Directory, that have not been updated in 90 days by default.



4. (Optional) The 90-day default can be set to a different default number of days used in the query. To do so, prior to clicking **Run**, click **View**.

   At the top of the page, select **Resource Purge SQL Executions** and amend the value in the **Show Parameters**.



5. When the query parameters are satisfactory, return to the task and click **Run**.

Scheduling Tasks

In addition to maintenance tasks, there are other tasks that should be scheduled to run regularly by Privilege Manager administrators. It's recommended to run these tasks to determine how long they take to complete in each environment, then schedule appropriately to cover task completion and needs.

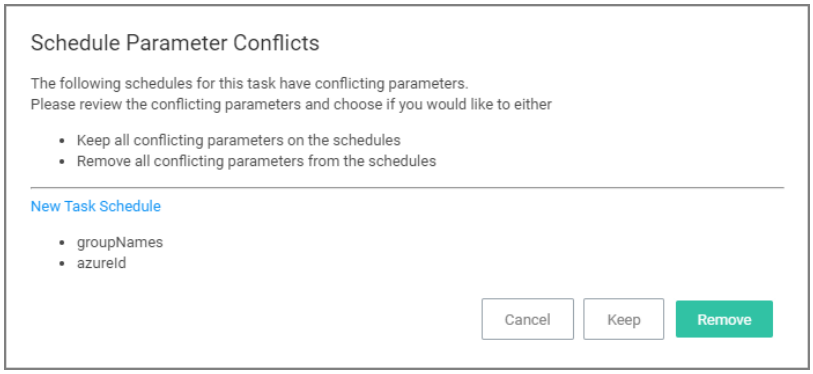
AD Import and Synchronization Tasks

Import Active Directory users and groups on demand and based on a set schedule.

Note: Depending on AD structure and size, the tasks should be planned to avoid bulk imports and synchronization of too large of a number of accounts.

Task Parameter Conflicts

When task parameters are set at the task level, they can't be changed when a schedule is created for that task. However, in some circumstances, if you have already defined parameters at the task schedule level and then go back to the task to set the values, you may end up with task schedule parameter conflicts. When there are conflicts with the version currently on the server, the Privilege Manager console shows a modal to resolve the existing conflicts before any schedule modifications can be saved.



The user can review the task that introduced the conflict by clicking the linked item, which is opened in a new browser tab.

The options to resolve are

- Keep all conflicting parameters on the schedule - click the **Keep** button.
- Remove all conflicting parameter from the schedule - click the **Remove** button.

Or, cancel if you wish to clean up the conflicts by manually editing task parameters on the conflicting items. However, something indicated as a conflict isn't necessarily a problem. The functionality is implemented so that users have the ability to stop changes on the schedule level by setting something other than default on the task level. If a parameter on the task is a default value, then that parameter will not be in conflict, if it does not match on the schedule.

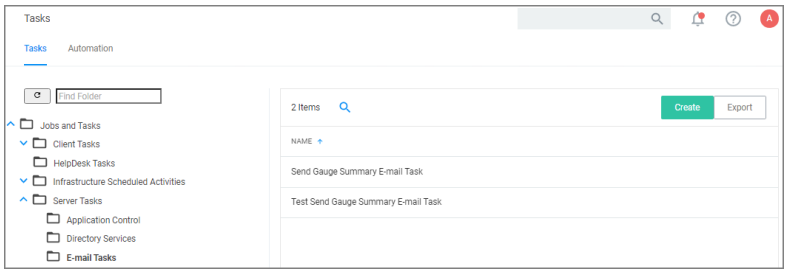
Whenever there is a deviation from the default value on the task level, even with the parameter on the schedule matching, users are asked to resolve the conflict by keeping the current values.

E-mail Reports Task

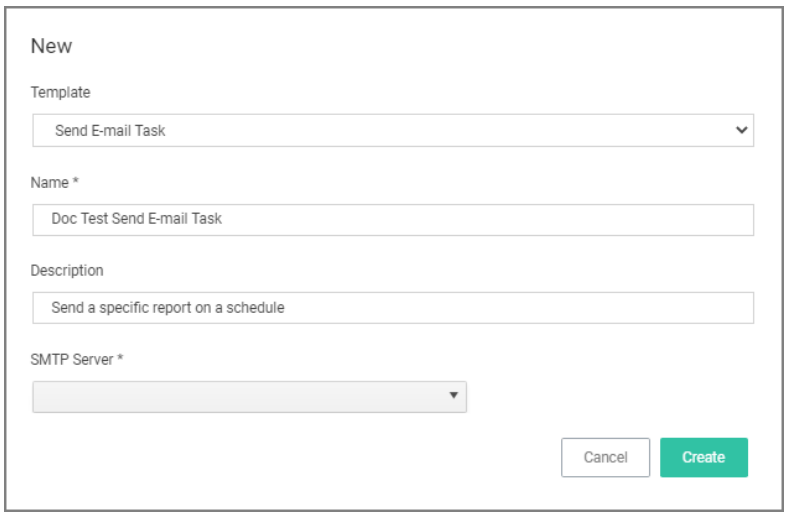
Any report created in Privilege Manager can be sent to a group of recipients based on a scheduled task.

To set this up, create a new Server task to send emails.

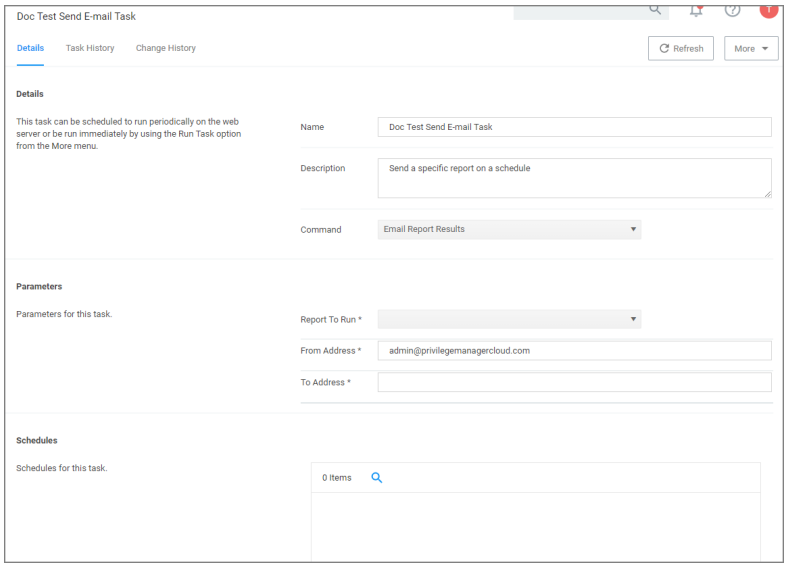
1. Navigate to **Admin | Tasks**.
2. In the folder tree open **Server Tasks | E-mail Tasks**.



3. Click **Create**. For on-prem instances the modal has an SMTP Server selection option, for cloud instances the server defaults to a pre-configured value and does not have the SMTP Server field.



4. From the Template drop-down select **Send E-mail Task**.
5. Enter the task name and description.
6. If this is for an on-premises instance, for **SMTP Server**, search for your SMTP server that is already configures as a foreign system for your instance.
7. Click **Create**.



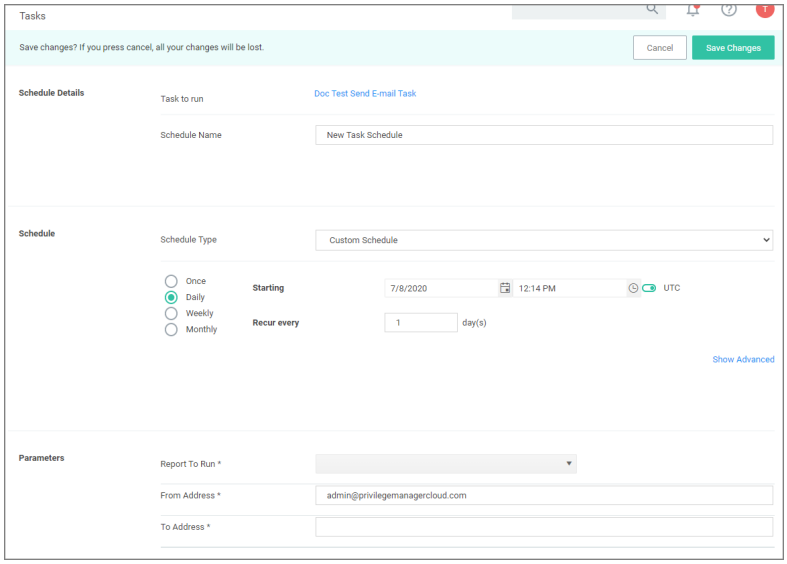
Note: For cloud environments the SMTP server settings are pulled from an existing configuration and can't be edited via the parameters tab.

Under **Details** and **Parameters** you can change/edit any of the task specific information:

1. From the **Command** drop-down, select what command you wish to execute, e.g. Email Report Results.
2. From the **Report to Run** drop-down, search for and select the report you wish to send.
3. In the **From Address** field enter the sender information you wish to be provided.
4. In the **To Address** field specify the recipient(s) (this can be a comma-separated list of addresses).
5. Click **Save Changes**.

Under the **Schedules** section of the page you can specify a schedule for this specific task.

1. Click **New Schedule**.



Set up the schedule specifics for this task.

2. Click **Save Changes**.

Server Tasks

Note: With Privilege Manager v11.2.0, UTC support on task schedules has been deprecated. Delinea recommends to disable UTC on any configured task schedules.

Component Based List of Default Tasks

Component	Task	Description
Application Control	Get Security Rating for File	Get/update the security rating for the given file.
	Get Security Ratings for Files	Get/update the security ratings for the given files.
	Refresh Security Rating Reports	Refreshes old security rating reports for resources rated by the given provider.
Application Control Cylance		
Email Tasks	Send Gauge Summary E-mail Task	Send a specific report on a schedule.

Component	Task	Description
File Inventory	Inventory File	Run this task to collect detailed information on the selected file for reports, filters, etc.
	Inventory File Resource	Run this task to update information on an existing file resource for reports, filters, etc.
	Inventory Package	Run this task to scan the contents of a package and report detailed information on files it contains for reports, filters, etc.
	Inventory Package with Exclusions	Run this task to scan the contents of a package and report detailed information on files it contains for reports, filters, etc.
	Inventory Packages	Run this task to scan the contents of a list of packages and report detailed information on files it contains for reports, filters, etc.
	Inventory Packages Referenced in Allow Lists	Run this task to collect detailed information for files contained in packages referenced in one or more allow lists.
	Inventory Uploaded File	This task is used internally to collect detailed information from files uploaded remotely to the server. It is visible only for status information and troubleshooting.
Foreign Systems		
	Refer to	Directory Services for details on the following Directory Services Tasks
Directory Services	Import Directory	Run this task to import/update directory OUs, users, and containers.
	Import Directory Computers	Run this task to import/update directory computer resources.
	Import Directory Sites	Run this task to import/update directory sites.
	Import Specific Azure AD Users and Groups	Import specific users and groups from Azure Active Directory.
	Synchronize Organizational Unit Server Task	Synchronize Organizational Unit Server Task.

Component	Task	Description
	Update OU Directory Scope Collections Membership	This task updates the membership of Directory Services OU scope collections.
	Update OU Directory Scope Collections Membership 2	This task updates the membership of Directory Services OU scope collections.
DS - Maintenance	Delete Imported Azure AD Resources	This task will delete users, groups, and devices from Privilege Manager that were imported from Azure AD.
	Refer to	Directory Services Maintenance for details on the following Directory Services Maintenance Tasks
	Delete Imported Directory Resources	This task will delete users, groups, computers, OUs, and Sites from Privilege Manager that were imported from AD.
	Merge Computers with Duplicate Azure Device IDs	This task will merge computers with duplicate Azure AD Device IDs.
	Merge Duplicate Account SID Resources	Run this task to merge resources that have a duplicate account SID.
	OU Directory Scope Collection Update	This task updates the membership of Directory Services OU scope collections based on a selected Schedule Type.
	Update OU Directory Scope Collections Membership	This task updates the membership of Directory Services OU scope collections.
	Update OU Directory Scope Collections Membership 2	This task updates the membership of Directory Services OU scope collections.
Obsolete	Import Azure Ad Users/Groups	This task is obsolete and should not be used anymore.

Component	Task	Description
	SCCM	Tasks here let you synchronize users, computers, and specific SCCM collection.
	ServiceNow	Creates ServiceNow Approval Request items.
	Symantec Management Platform	Tasks here let you synchronize SMP collections and package(s).
	Syslog	Creates tasks to send events to the configured syslog server based on specific templates.
Local Security	Update Primary User	Updates the primary user for the given computer resource.
	Update Primary User for Collection	Updates the primary user for each computer in the given collection.
Thycotic One Users	Sync users with Thycotic One	Run this task to synchronize PM users with a Thycotic One instance.
Security	Rebuild Item Security Cache	Run this task to mark all entries in the item security cache as invalid, forcing a rebuild.
	Refresh Agent Secrets	Run this task to refresh the agent secrets that were generated before the given max age.
	Revoke Agent Secrets	Run this task to revoke the secrets from one or more agents.
	Revoke Secrets from All Agents	Run this task to revoke the secrets from all agents.
	Set Security Rating	Run this task to manually set the security rating (used in filters) for the selected files.
	Update Security Ratings for Resource	Run this task to update the security ratings (used in filters) for the given resources using the given rating system.
Utility	Delete Item	This task will delete an item, and optionally dependent children.
	Reset Licensing	This task will reset licensing, deleting all installed license keys.

Component	Task	Description
	Update Server Gauge State	This task will update the state of a server gauge.
	Merge Duplicate Resources	This task will identify and merge Computers, Domain Users and Domain Groups with duplicate attributes, based on the Auto-Merge Computer settings in the Advanced Configuration.
	Merge Specific Resources	This task will merge one or more resources into a selected target resource, regardless of whether they have any duplicate data.

Directory Services Maintenance Tasks

The tasks in this component all help with the maintenance of directory services resources. These tasks are read-only items that need to be duplicated for any task customization.

You find the tasks when you:

1. Navigate to **Admin | Tasks**.
2. On the Tasks tab under Jobs and Tasks, select **Server Tasks**.
3. Select **Foreign Systems | Directory Services**.
4. Select **Maintenance**.

Delete Imported Azure AD Resources

This task will delete users, groups, and devices from Privilege Manager that were imported from Azure AD.

Parameters

- Directory: The Azure AD instance from which to delete resources.
- Delete users: If set, then this task will delete users from Privilege Manager imported from the given directory.
- Delete groups: If set, then this task will delete groups from Privilege Manager imported from the given directory.
- Delete devices: If set, then this task will delete computers and other devices from Privilege Manager imported from the given directory.
- Ignore dependencies: Use this as a last resort if you wish to delete and ignore any items that depend on the resources being deleted.

Delete Imported Directory Resources

This task will delete users, groups, computers, OUs, and Sites from Privilege Manager that were imported from AD.

Parameters

- Directory: The AD instance from which to delete resources.
- Delete users: If set, then this task will delete users from Privilege Manager imported from the given directory.

- Delete groups: If set, then this task will delete groups from Privilege Manager imported from the given directory.
- Delete computers: If set, then this task will delete computers from Privilege Manager imported from the given directory.
- Delete organization: If set, then this task will delete OUs from Privilege Manager imported from the given directory.
- Delete sites: If set, then this task will delete sites from Privilege Manager imported from the given directory.
- Ignore dependencies: Use this as a last resort if you wish to delete and ignore any items that depend on the resources being deleted.

Merge Computers with Duplicate Azure Device IDs

This task will merge computers with duplicate Azure AD Device IDs.

Parameters

- Directory: The Azure AD instance from which to merge resources. Leave empty for all.

Merge Duplicate Account SID Resources

Run this task to merge resources that have a duplicate account SID.

Parameters

- Target Resources: Leave empty to automatically discover all. Select only the target, not its duplicates. Any resources with SID matching a target will be merged into the target.

OU Directory Scope Collection Update

This task updates the membership of Directory Services OU scope collections based on a selected Schedule Type.

Update OU Directory Scope Collections Membership

This task updates the membership of Directory Services OU scope collections.

Parameters

- Directory collections: The set of directory collections whose membership will be updated.

Update OU Directory Scope Collections Membership 2

This task updates the membership of Directory Services OU scope collections.

Parameters

This task has a **Force all** parameter that forces the membership of all directory scope collections to update, regardless of an update required detection.

Directory Services Tasks

The directory services tasks in this component cover different types of directory services imports.

You find the tasks when you:

1. Navigate to **Admin | Tasks**.
2. On the Tasks tab under Jobs and Tasks, select **Server Tasks**.
3. Select **Foreign Systems | Directory Services**.

Import Azure AD Resources

This task will import devices, users, and groups from Azure AD.

Parameters

- Directory: The Azure AD instance from which to import/synchronize.
- Import Users: If set, then this task will search for users in the given Azure AD instance.
- Import Groups: If set, then this task will search for groups in the given Azure AD instance.
- Import Devices: If set, then this task will search for devices in the given Azure AD instance.
- Create users when not matched: If set, then users not matched to an existing resource in Privilege Manager will be created.
- Create groups when not matched: If set, then groups not matched to an existing resource in Privilege Manager will be created.
- Create devices when not matched: If set, then devices not matched to an existing resource in Privilege Manager will be created.

  Note: Devices are particularly vulnerable to duplication due to the lack of identifiers in Azure AD. Refer to Best Practices for AD Imports for details.

Import Directory Computers

Run this task to import/update computers and their OUs.

Parameters

- Directory Id: The directory Id from which to import/synchronize. This is the only required parameter for this task.
- Directory partner Id:
- Full sync:
- Query: Where the object class = the computer.
- Search configuration:

Import Directory Sites

Run this task to import/update directory sites.

Parameters

- Directory Id: The directory Id from which to import/synchronize. This is the only required parameter for this task.
- Directory partner Id:
- Full sync:
- Query: Where the object class = the site.
- Search configuration:

Import Directory Users and Groups

Run this task to import/update users, groups, and their OUs.

Parameters

- Directory Id: The directory Id from which to import/synchronize. This is the only required parameter for this task.
- Directory partner Id:
- Full sync:
- Query: Where the object class = the site.
- Search configuration:

Import Directory OU

Run this task to import resources from a specific Directory Services OU.

Parameters

- Organization Unit:

Import Specific Azure AD Users and Groups

This task will import the specified users, devices, groups, and optionally child groups, users, and devices from Azure AD.

Parameters

- Azure AD: The Azure AD instance from which to import/synchronize.
- Create groups when not matched (no): If set, then devices not matched to an existing resource in Privilege Manager will be created.

  Note: Devices are particularly vulnerable to duplication due to the lack of identifiers in Azure AD. Refer to Best Practices for AD Imports for details.
- Create groups when not matched (yes): If set, then groups not matched to an existing resource in Privilege Manager will be created.
- Create users when not matched: If set, then users not matched to an existing resource in Privilege Manager will be created.

- Device names: The display names of the devices to import. Leave empty for none. Use a newline between names. End name with '*' to find all that start with the given name.
- Group display names: The display names of the groups to import. Leave empty for none. Use a newline between names. End name with '*' to find all that start with the given name.
- Import child devices: If set, then child devices of any discovered group will be imported.
- Import child users: If set, then child users of any discovered group will be imported.
- Recurse child groups: If set, then child groups of the given group names will be imported recursively.
- User names: The display names or user principal names (UPN) of the users to import. Leave empty for none. Use a newline between names. End name with '*' to find all that start with the given name.

Merge Duplicate Resources

This task will identify and merge Computers, Domain Users and Domain Groups with duplicate attributes, based on the **Auto-Merge Computer** settings in the Advanced Configuration.

Merge Specific Resources

This task will merge user defined Computers, Domain Users and Domain Groups with duplicate attributes, based on the **Auto-Merge Computer** settings in the Advanced Configuration.

Server Tasks

Note: With Privilege Manager v11.2.0, UTC support on task schedules has been deprecated. Delinea recommends to disable UTC on any configured task schedules.

Component Based List of Default Tasks

Component	Task	Description
Application Control	Get Security Rating for File	Get/update the security rating for the given file.
	Get Security Ratings for Files	Get/update the security ratings for the given files.
	Refresh Security Rating Reports	Refreshes old security rating reports for resources rated by the given provider.
Application Control Cylance		
Email Tasks	Send Gauge Summary E-mail Task	Send a specific report on a schedule.

Component	Task	Description
File Inventory	Inventory File	Run this task to collect detailed information on the selected file for reports, filters, etc.
	Inventory File Resource	Run this task to update information on an existing file resource for reports, filters, etc.
	Inventory Package	Run this task to scan the contents of a package and report detailed information on files it contains for reports, filters, etc.
	Inventory Package with Exclusions	Run this task to scan the contents of a package and report detailed information on files it contains for reports, filters, etc.
	Inventory Packages	Run this task to scan the contents of a list of packages and report detailed information on files it contains for reports, filters, etc.
	Inventory Packages Referenced in Allow Lists	Run this task to collect detailed information for files contained in packages referenced in one or more allow lists.
	Inventory Uploaded File	This task is used internally to collect detailed information from files uploaded remotely to the server. It is visible only for status information and troubleshooting.
Foreign Systems		
	Refer to	Directory Services for details on the following Directory Services Tasks
Directory Services	Import Directory	Run this task to import/update directory OUs, users, and containers.
	Import Directory Computers	Run this task to import/update directory computer resources.
	Import Directory Sites	Run this task to import/update directory sites.
	Import Specific Azure AD Users and Groups	Import specific users and groups from Azure Active Directory.
	Synchronize Organizational Unit Server Task	Synchronize Organizational Unit Server Task.

Component	Task	Description
	Update OU Directory Scope Collections Membership	This task updates the membership of Directory Services OU scope collections.
	Update OU Directory Scope Collections Membership 2	This task updates the membership of Directory Services OU scope collections.
DS - Maintenance	Delete Imported Azure AD Resources	This task will delete users, groups, and devices from Privilege Manager that were imported from Azure AD.
	Refer to	Directory Services Maintenance for details on the following Directory Services Maintenance Tasks
	Delete Imported Directory Resources	This task will delete users, groups, computers, OUs, and Sites from Privilege Manager that were imported from AD.
	Merge Computers with Duplicate Azure Device IDs	This task will merge computers with duplicate Azure AD Device IDs.
	Merge Duplicate Account SID Resources	Run this task to merge resources that have a duplicate account SID.
	OU Directory Scope Collection Update	This task updates the membership of Directory Services OU scope collections based on a selected Schedule Type.
	Update OU Directory Scope Collections Membership	This task updates the membership of Directory Services OU scope collections.
	Update OU Directory Scope Collections Membership 2	This task updates the membership of Directory Services OU scope collections.
Obsolete	Import Azure Ad Users/Groups	This task is obsolete and should not be used anymore.

Component	Task	Description
	SCCM	Tasks here let you synchronize users, computers, and specific SCCM collection.
	ServiceNow	Creates ServiceNow Approval Request items.
	Symantec Management Platform	Tasks here let you synchronize SMP collections and package(s).
	Syslog	Creates tasks to send events to the configured syslog server based on specific templates.
Local Security	Update Primary User	Updates the primary user for the given computer resource.
	Update Primary User for Collection	Updates the primary user for each computer in the given collection.
Thycotic One Users	Sync users with Thycotic One	Run this task to synchronize PM users with a Thycotic One instance.
Security	Rebuild Item Security Cache	Run this task to mark all entries in the item security cache as invalid, forcing a rebuild.
	Refresh Agent Secrets	Run this task to refresh the agent secrets that were generated before the given max age.
	Revoke Agent Secrets	Run this task to revoke the secrets from one or more agents.
	Revoke Secrets from All Agents	Run this task to revoke the secrets from all agents.
	Set Security Rating	Run this task to manually set the security rating (used in filters) for the selected files.
	Update Security Ratings for Resource	Run this task to update the security ratings (used in filters) for the given resources using the given rating system.
Utility	Delete Item	This task will delete an item, and optionally dependent children.
	Reset Licensing	This task will reset licensing, deleting all installed license keys.

Component	Task	Description
	Update Server Gauge State	This task will update the state of a server gauge.
	Merge Duplicate Resources	This task will identify and merge Computers, Domain Users and Domain Groups with duplicate attributes, based on the Auto-Merge Computer settings in the Advanced Configuration.
	Merge Specific Resources	This task will merge one or more resources into a selected target resource, regardless of whether they have any duplicate data.

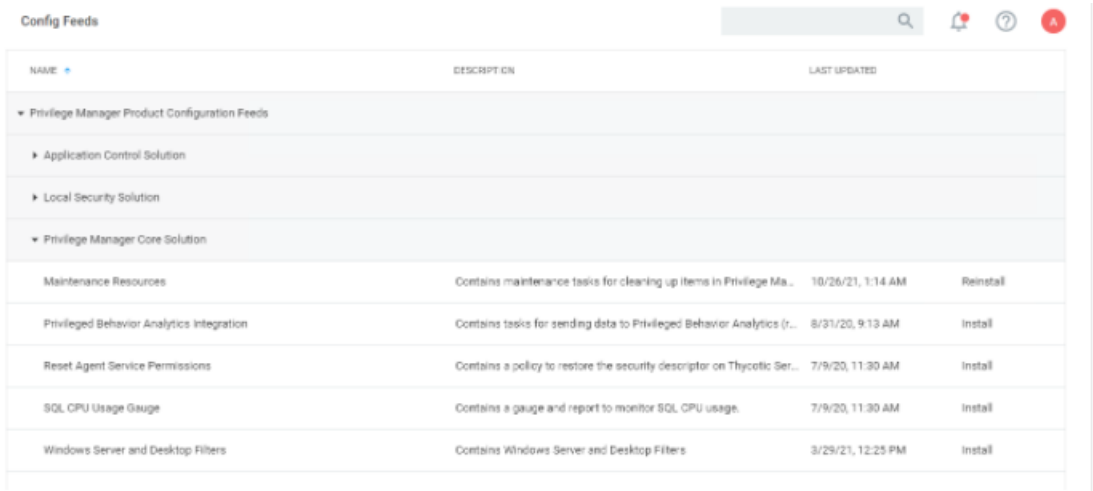
Tools Menu

The Tools menu in Privilege Manager offers access to

- Disclose Password
- File Upload
- Manage Approvals
- Offline Approvals
- Secret Server, if integrated.

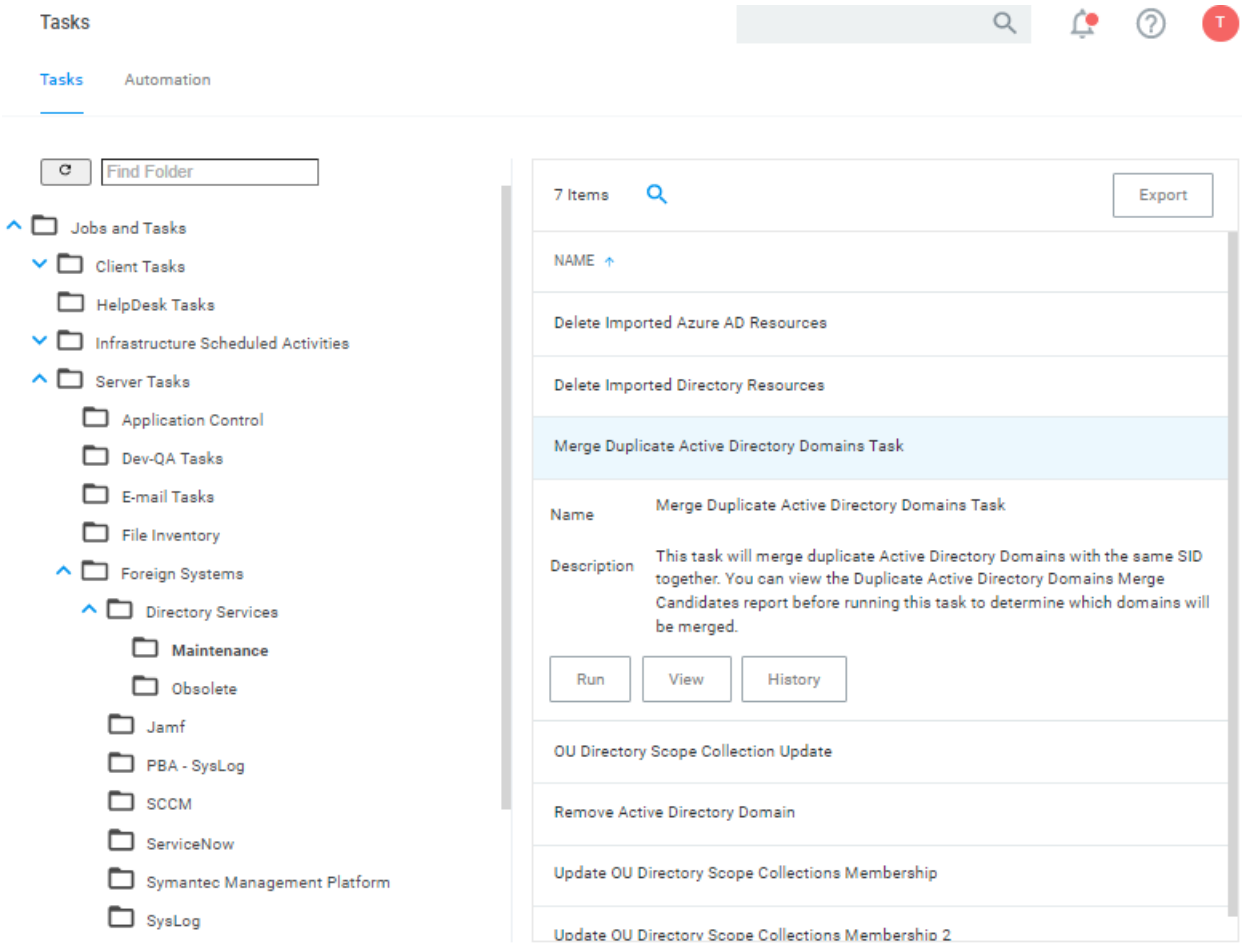
Merge Duplicate Active Directory Domains

1. Navigate to **Admin | Config Feeds**.
2. From the **Privilege Manager Product Configuration Feeds | Privilege Manager Core Solution**, install the **Maintenance Resource**.



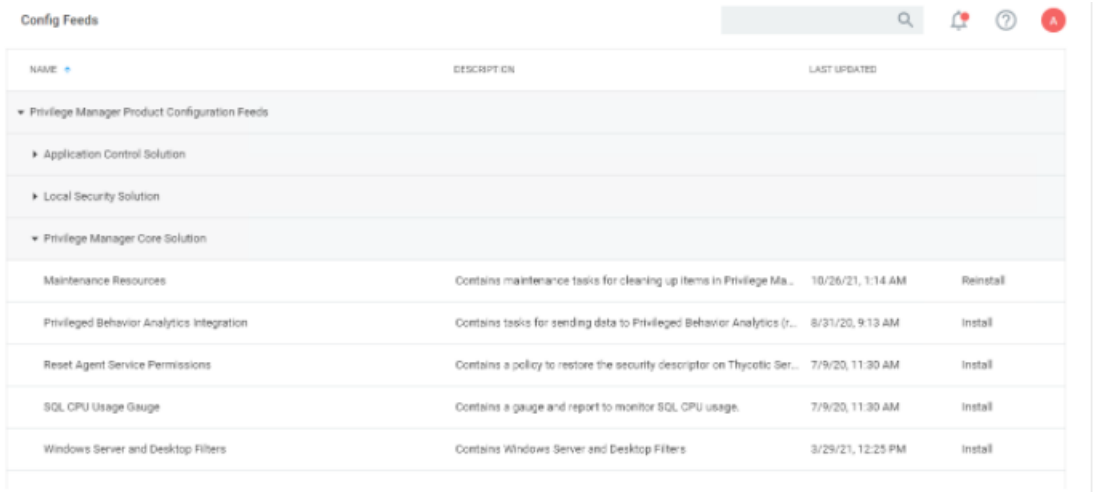
3. Navigate to **Reports**.

4. From the **Diagnostics** section, select **Duplicate Active Directory Domain Merge Candidates**. Identify the existing rows that require merging.
5. To merge domains, navigate to **Admin | Tasks**.
6. Expand **Server Tasks**.
7. Select **Foreign Systems | Directory Services | Maintenance**.
8. Select and run **Merge Duplicate Active Directory Domains**.

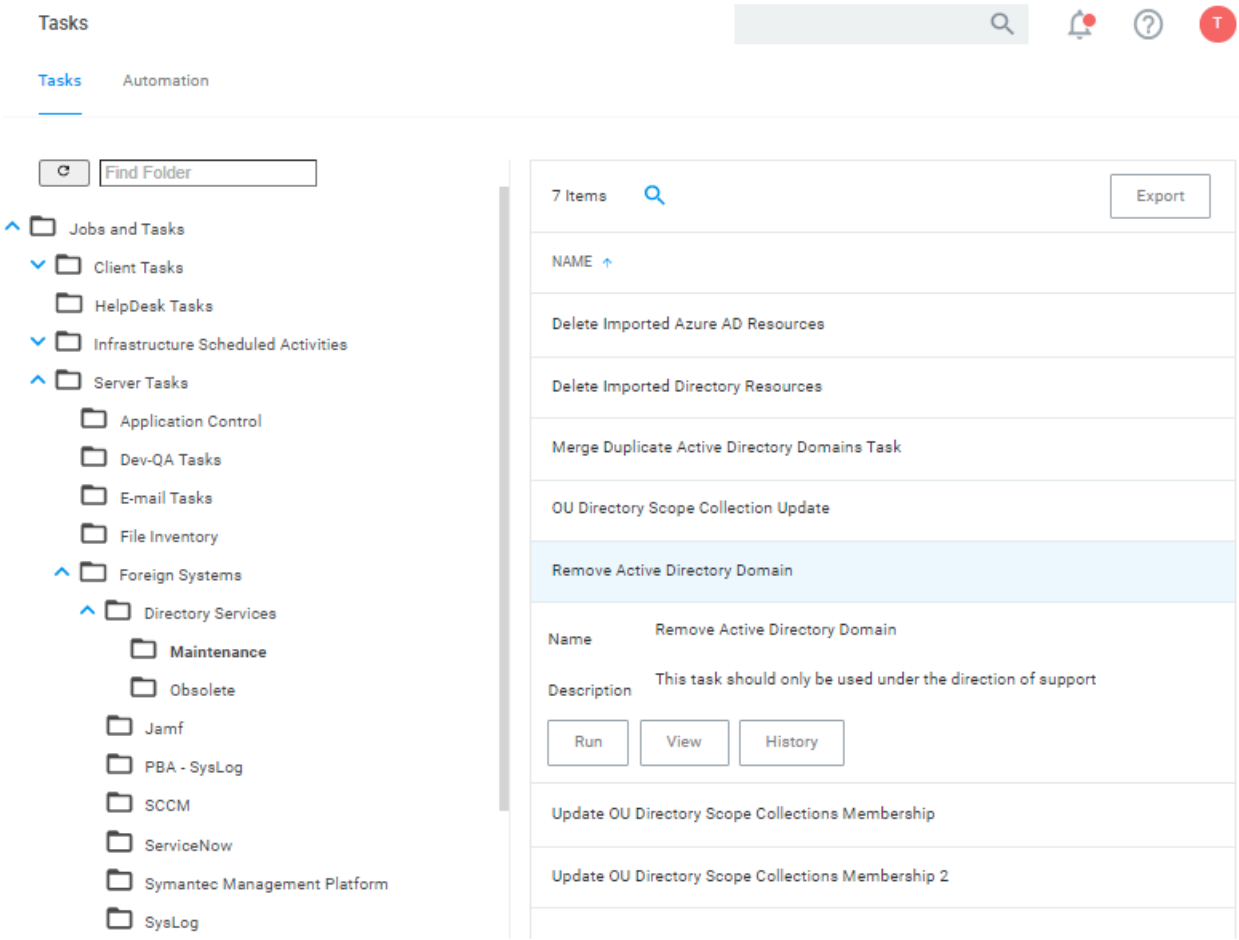


Remove Active Directory Domain

1. Navigate to **Admin | Config Feeds**.
2. From the **Privilege Manager Product Configuration Feeds | Privilege Manager Core Solution**, install the **Maintenance Resource**.



3. Following the installation, navigate to **Admin | Tasks**.
4. Expand **Jobs and Task | Server Tasks**.
5. Under **Foreign Systems | Directory Services | Maintenance**, select and run **Remove Active Directory Domain**.



Tools Menu

The Tools menu in Privilege Manager offers access to

- Disclose Password
- File Upload
- Manage Approvals
- Offline Approvals
- Secret Server, if integrated.

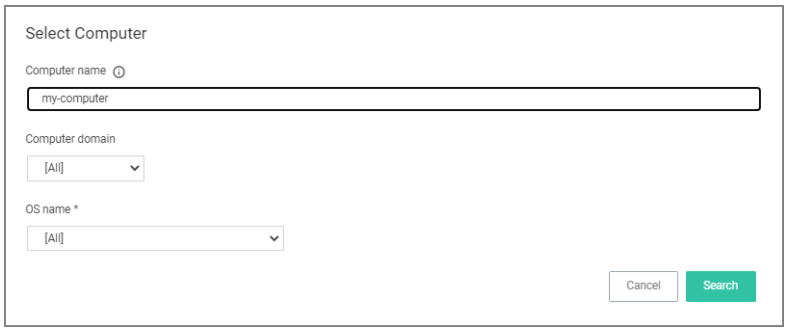
Password Disclosure

The Password Disclosure tool lets users based on role permissions disclose passwords and look a password rotation history.

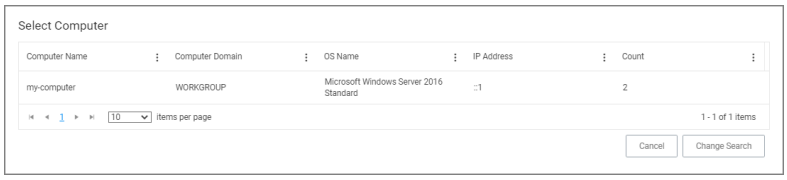
The password rotation history is helpful when systems are being restored to a time prior to the current password.

Using the Disclose Password Tool

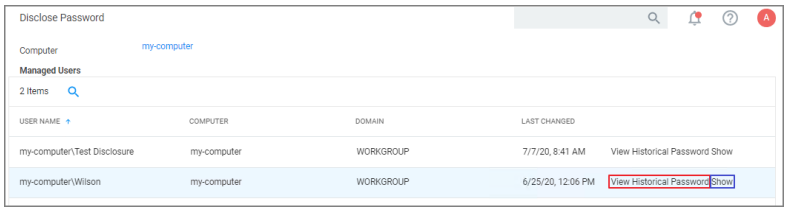
1. Navigate to **Admin | Tools: Disclose Password**.
2. The Computer page opens.



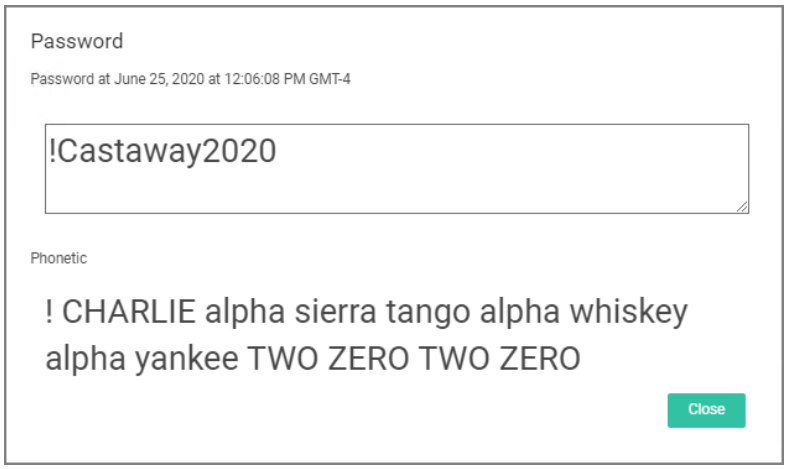
Select a computer from the list.



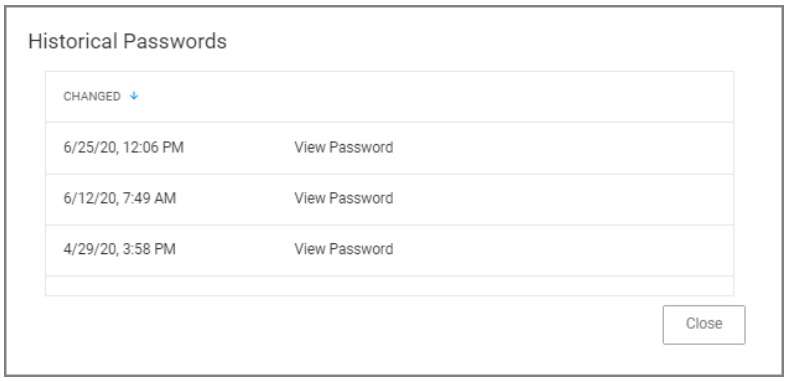
3. The Password Disclosure page opens, it list the managed users and also provides links to view the current password and to password history.



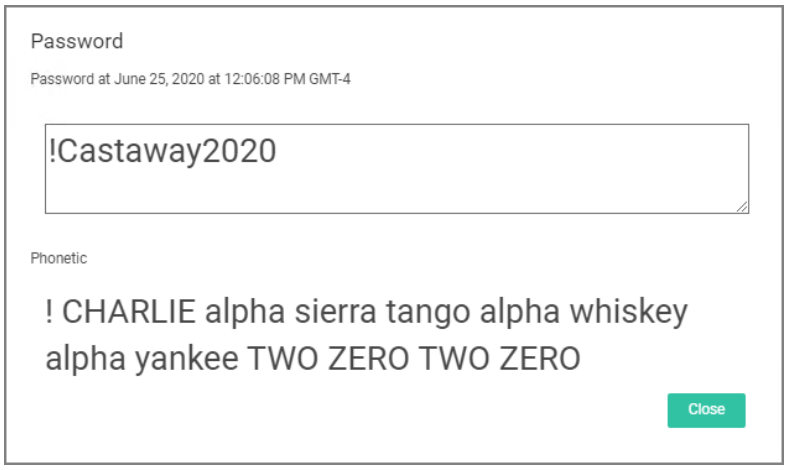
4. Click on **Show** to view the current password.



5. Click on **View Historical Password** to view the password history.



Select a link on the **Historical Password** modal to view any of the rotated passwords.



Note: Any password disclosure is audited and can be viewed in the **Password Disclosure History** report (requires Administrator role membership).

Users

Administrator users can create and edit Privilege Manager users and assign and remove roles for these users.

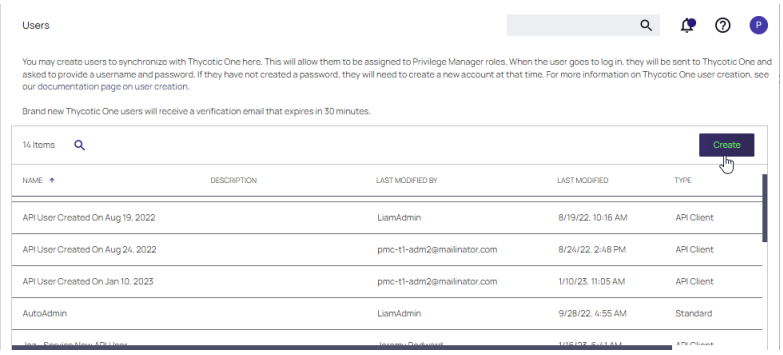
There are three types of users:Thycotic One

- users - these are only available in cloud environments and are manually added.
- API Users - these are available for the public API implementation.
- Standard Users - these are users manually added by an administrator after the initial installation of Privilege Manager.
- Federated Users - these are users, whose identity is linked across multiple security domains. They authenticate with one and can access resources in the other.

How to Manually Add Thycotic One Users

To manually add users to your Privilege Manager cloud instance, follow these steps:

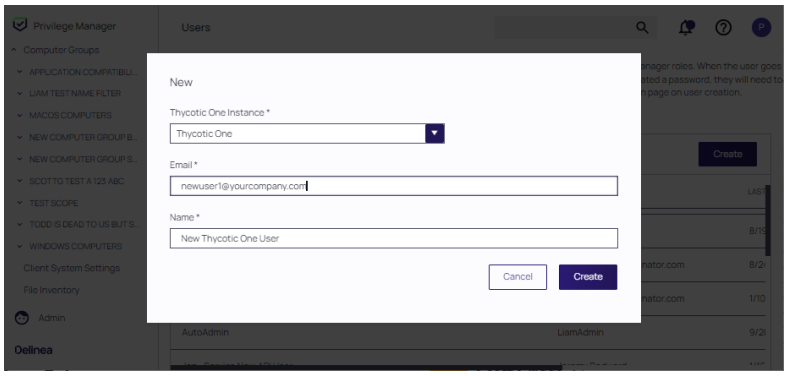
1. Navigate to **Admin | Users**. Click **Create**.



2. At the **Select a User Type** dialog, select **Thycotic One** as the user type and click **Create**.

3. The **New** dialog displays. Provide information for the new user.
   - From the **Thycotic One Instance** drop-down, search for and select your instance for the new user.
   - Enter the **Email** and **Name** of the new Thycotic One user in the respective fields.

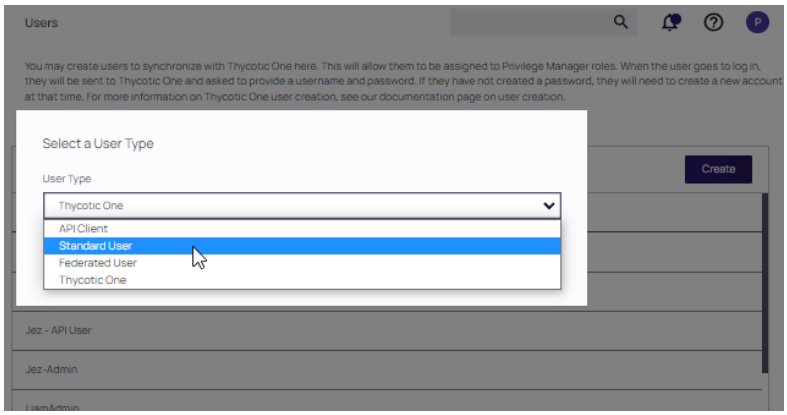
   Click **Create**.



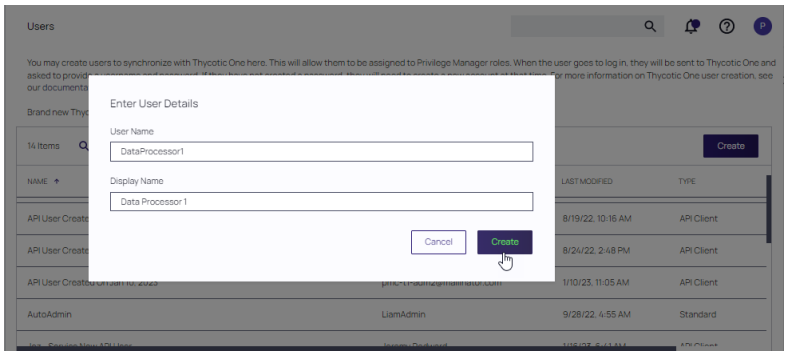
How to Manually Add Standard Users

Standard users can view and edit their own accounts, such as password updates, but can't create new users or delete their own user.

1. Navigate to **Admin | User**. On-prem instances see a note that Thycotic One users can only be created if a Thycotic One Foreign System is configured.
2. Click **Create**.
3. From the **User Type** drop-down, select **Standard User** and click **Create**.

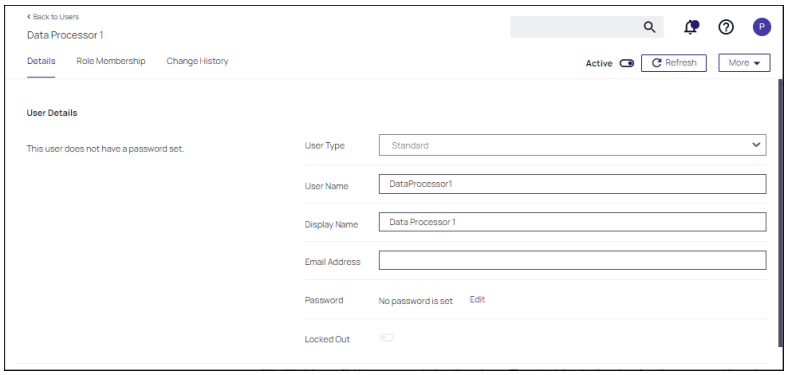


4. On the **Enter User Details** modal, enter the **User Name** and the **Display Name**. Click **Create**.



5. On the newly created User Details page, supply a user type, user name, display name, email address, and password (click *Edit_* to define). **Locked Out** is used to reset the user account if the user becomes locked out.

   Click **Save Changes**.

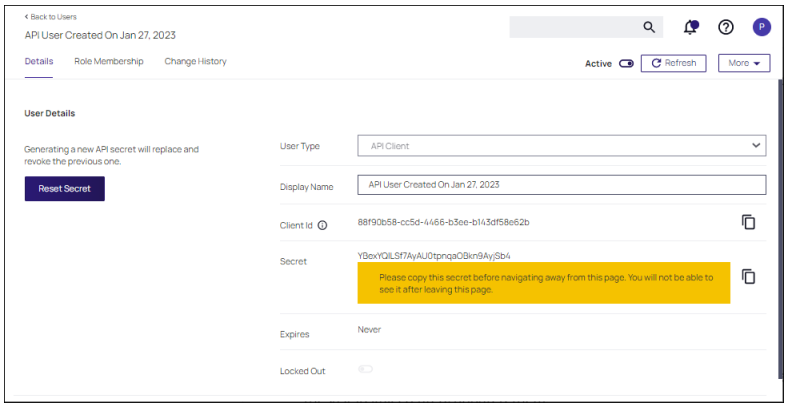


The user is now active in the system and you may edit the user details.

How to Manually Add API Client Users

API Client users can view and edit their own accounts, such as password updates, but can't create new users or delete their own user.

1. Navigate to **Admin | User**. Click **Create**.
2. From the **User Type** drop-down select **API Client** and click **Create**.



API Client users are by default created with a date and time reference when the user was added. If you wish, you can modify the display name. The newly create user is automatically set to active on creation. Prior to navigating away from the page, make sure to take note of the **Client ID** and copy the **Secret** into your vault.

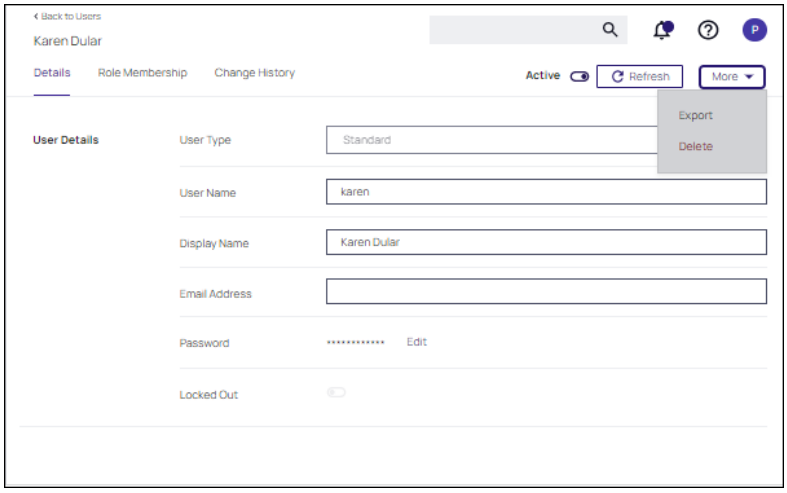
Make sure the API user is a member of a role, the role depends on what you need the API to do.

Use **Reset Secret** to generate a new secret for this user, it invalidates the old secret you copied to the vault. Once you click **Reset Secret** you need to confirm the action. The new secret will be shown until you navigate away from the page. All changes need to be saved to take effect.

Editing, Deleting, and Exporting a User

Select an existing user on the Users page. The User details page displays, where you can:

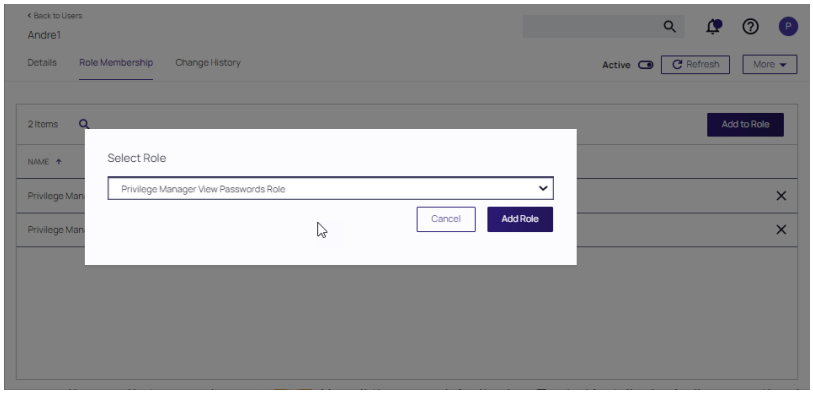
- Edit **User Details**.
- Select **Delete** at the **More** pull-down to delete the user.
- Select **Export** at the **More** pull-down to download a ZIP file of the user and children.



Note: Thycotic One user accounts created prior to v11.4.0 need updates to their XML in order to have the **Delete** option available in the user interface. Refer to Deleting a Thycotic One Account (pre v11.4.0).

Role Membership

The **Role Membership** tab allows administrators to verify existing role memberships for any given Privilege Manager user. Administrators can also remove any roles via the **X** on the table grid and add users to a role via **Add to Role** options.



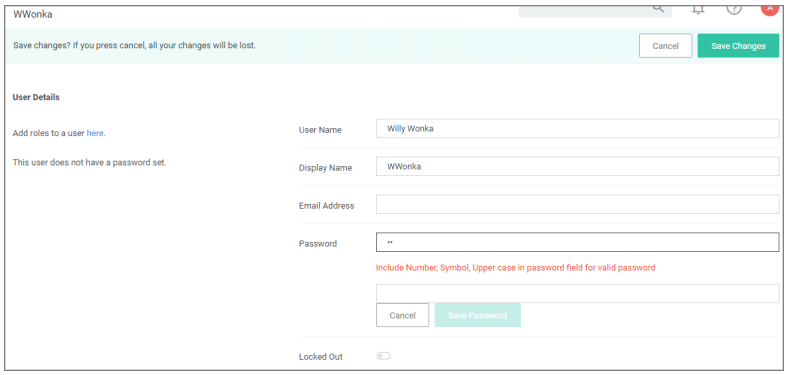
1. Click **Add to Role**
2. Select a role at the **Select Role** drop-down and click **Add Role**.

Password Complexity Enforcement

Privilege Manager Administrators can turn complex password policy rules on and off for Privilege Manager users. This can be set via the advanced configuration page. Password complexity is turned on by default.

Policy rules:

- minimum of 8 characters
- minimum 1 symbol
- minimum 1 uppercase
- minimum 1 lowercase



The password policy applies to UI and API Client users.

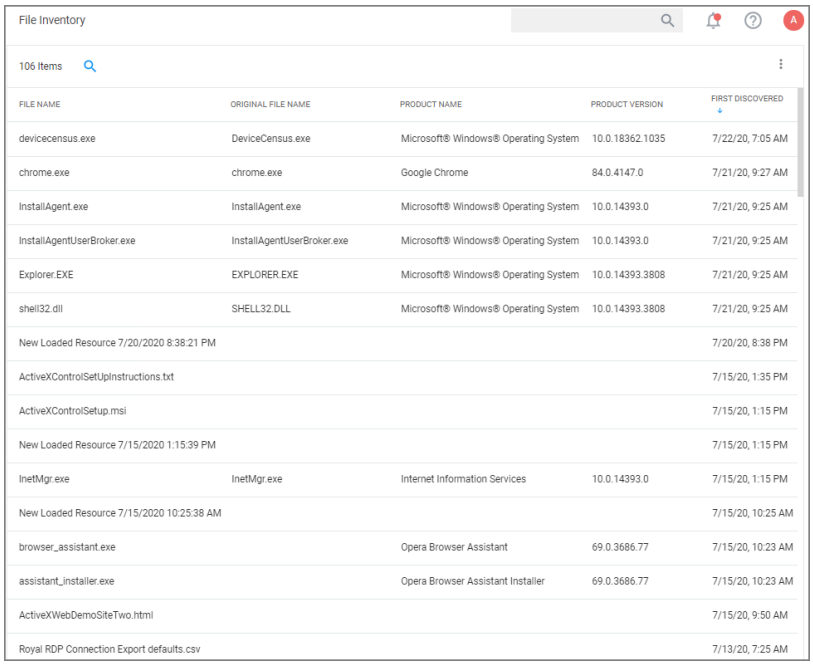
The enforcement takes effect when a new Privilege Manager user is created or an existing user resource is edited.

File Inventory

The file inventory page lists all files discovered based on the Basic Inventory policies.

The table grid contains the following columns:

- File Name
- Original File Name
- Product Name
- Product Version
- First Discovered



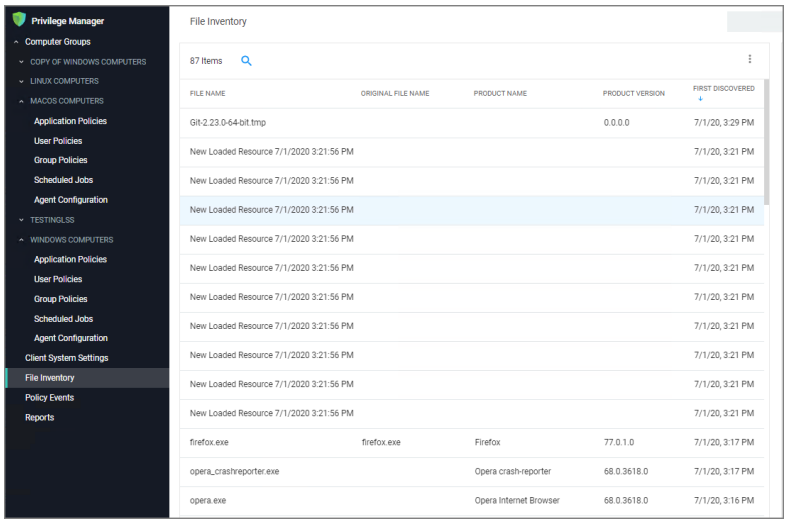
File Inventory

106 Items

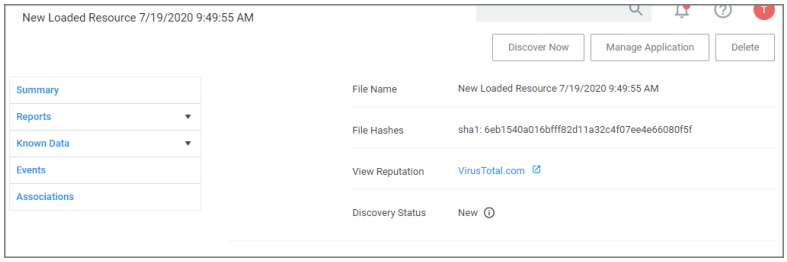
FILE NAME	ORIGINAL FILE NAME	PRODUCT NAME	PRODUCT VERSION	FIRST DISCOVERED
devicecensus.exe	DeviceCensus.exe	Microsoft® Windows® Operating System	10.0.18362.1035	7/22/20, 7:05 AM
chrome.exe	chrome.exe	Google Chrome	84.0.4147.0	7/21/20, 9:27 AM
InstallAgent.exe	InstallAgent.exe	Microsoft® Windows® Operating System	10.0.14393.0	7/21/20, 9:25 AM
InstallAgentUserBroker.exe	InstallAgentUserBroker.exe	Microsoft® Windows® Operating System	10.0.14393.0	7/21/20, 9:25 AM
Explorer.EXE	EXPLORER.EXE	Microsoft® Windows® Operating System	10.0.14393.3808	7/21/20, 9:25 AM
shell32.dll	SHELL32.DLL	Microsoft® Windows® Operating System	10.0.14393.3808	7/21/20, 9:25 AM
New Loaded Resource 7/20/2020 8:38:21 PM				7/20/20, 8:38 PM
ActiveXControlSetUpInstructions.txt				7/15/20, 1:35 PM
ActiveXControlSetup.msi				7/15/20, 1:15 PM
New Loaded Resource 7/15/2020 1:15:39 PM				7/15/20, 1:15 PM
InetMgr.exe	InetMgr.exe	Internet Information Services	10.0.14393.0	7/15/20, 1:15 PM
New Loaded Resource 7/15/2020 10:25:38 AM				7/15/20, 10:25 AM
browser_assistant.exe		Opera Browser Assistant	69.0.3686.77	7/15/20, 10:23 AM
assistant_installer.exe		Opera Browser Assistant Installer	69.0.3686.77	7/15/20, 10:23 AM
ActiveXWebDemoSiteTwo.html				7/15/20, 9:50 AM
Royal RDP Connection Export defaults.csv				7/13/20, 7:25 AM

At the beginning of your policy creation process you will see many new events labeled as **New Loaded Resource**. This is because importing files in Privilege Manager is not the same thing as discovering information about the files. Discovery of file details is done by scheduled tasks by default, but if you want to discover file details immediately, do the following:

1. Navigate to **File Inventory**.
2. Select **New Loaded Resource**.



3. Click on a **New Loaded Resource** entry.



   a. Check the Discover Status. The following states are available:
      - **New**, the resource was just reported).
      - **Pending Assignment**, the resource will soon be assigned to an agent for discovery).
      - **Assigned to agent**, an agent was chosen to discover this resource.

      Once an agent is assigned, you can click **Discover Now** to attempt to force the agent to immediately discover the resource. Many factors affect the agent's promptness in discovering the resource: agent up-time, current processing queue, etc. Please be patient.

4. Click **Discover Now**.
5. After the successful discovery, click **View File** or **Create Filter** as your next option to use the discovered or inventoried resource. You have the option to add it to a Policy.

Note: Files may not be discovered if they have already been deleted from your system.

Privilege Manager API

Delinea is following the OpenAPI standard and our customers are offered the standard Swagger UI interface to interact with and learn how to use Privilege Manager's public API endpoints.

Installing the API

The Privilege Manager Application Programming Interface packages are installed through the main Privilege Manager console. Navigate to **Admin | Setup** and follow the steps as documented under Upgrades

> **Note:** Cloud instances have the API installed by default, just like other features, such as foreign system connectors, etc.

Creating an API Client User

Before you can access the API and start using the API endpoints, you need to setup an API Client User in the Privilege Manager Console. For details on the API Client User setup refer to the Users topic in the main Privilege Managerdocumentation, specifically access How to Manually Add API Client Users and the Add Roles to a User information.

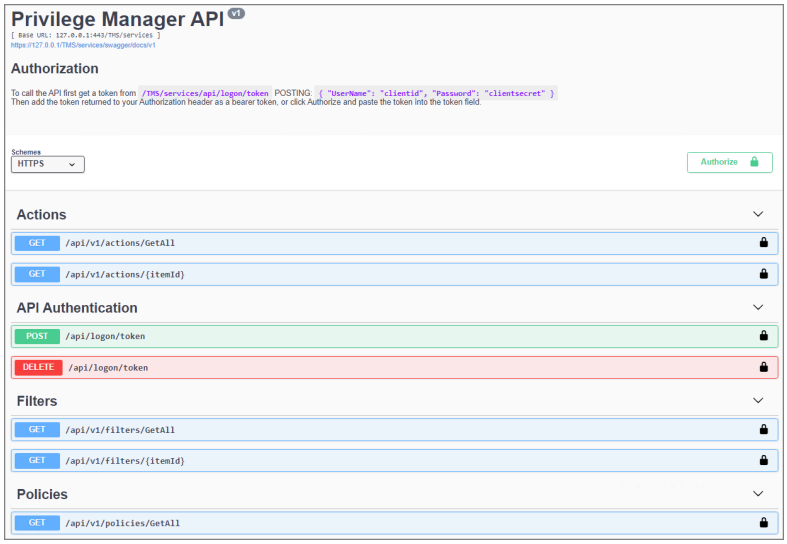
Refer to the Security and Application Roles topics to learn more about the type of roles required to execute tasks in Privilege Manager. For example, to make changes to policies, that API Client User needs to be added to an administrator role (macOS, Windows, or full Privilege Manager Admin). To simply read a policy, filter, or action, the Privilege Manager Users role is sufficient.

Accessing the API

To access the Privilege Manager API,

1. In the Privilege Manager Console in the upper right-hand corner of the page, navigate to the **Help** icon.
2. Select **API Reference**. The standard URL to your API is for

   on-prem: `https://myserver.example.com/Tms/services/swagger/ui/index`
   cloud:`https://mycompany.privilegemanagercloud.com/Tms/services/swagger/ui/index`



API Authentication

To call the API first user need to get a token from `.../Tms/services/api/logon/token`.

Refer to these scripts for examples:

- Authentication with invoke REST method
- Authentication with invoke web request
- Get Token with invoke REST method
- Get Token with invoke web request

POST

You will need to post a request message with the following details:

```
POST /api/logon/token
{
  "Password": "string",
  "UserName": "string"
}
```

Parameter	Value
Password	clientsecret
UserName	clientid

The auth token will be returned to you.

1. Copy the token.
2. Click **Authorize**.
3. In the **Available authorizations** modal, paste that token into the **Value** field.
4. On the modal click **Authorize**.

You may also add the returned token to your Authorization header as a bearer token.

Refer to "How to Manually Add API Client Users" and "Add Roles to a User" to setup your API Client User and to add that user to the Privilege Manager Administrators role.

DELETE

For an API Client User to logout, a DELETE request for the api/logon/token needs to be issued with the bearer token in the Authorization header.

```
curl -X DELETE --header "Authorization: Bearer {token}"
"https://yourinstancename/tms/services/api/logon/token"
```

with a request URL of:

`https://yourinstancename/TMS/services/api/logon/token`

Privilege Manager Mobile Application

The Privilege Manager Mobile console allows you to process approval requests, disclose passwords, and view alerts via the Privilege Manager Mobile Application on iOS and Android smartphones.

Prerequisites

- Perform Azure AD synchronization
- Include "Mobile Message Approval Process" as a user role

Next, you must:

- Install the Privilege ManagerMobile Console
- Set up Azure AD such that you can add an application registration
- Configure the Microsoft Azure Service Bus
- Install the Privilege ManagerMobile Application

These instructions are based on the following assumptions:

1. The customer is using Azure AD and has already configured the Azure Active Directory App Registration per the documentation, allowing the customer to authenticate as an Azure AD user. The mobile application registration is added to the **same domain**.
2. The customer has the ability to create an Azure Service Bus service.

Detailed Instruction Topics

To begin the Privilege ManagerMobile Console setup, review the topics below (in the sequence listed) and follow all instructions:

1. Add the mobile application registration to your Azure Active Directory integration with Privilege Manager
2. Configure the Service Bus for Mobile
3. Install and Configure the Privilege Manager Mobile Console Solution on the Privilege Manager Server
4. Install the Privilege Manager Mobile App on a Mobile Device
5. Use the Mobile Application

Configure Azure Active Directory

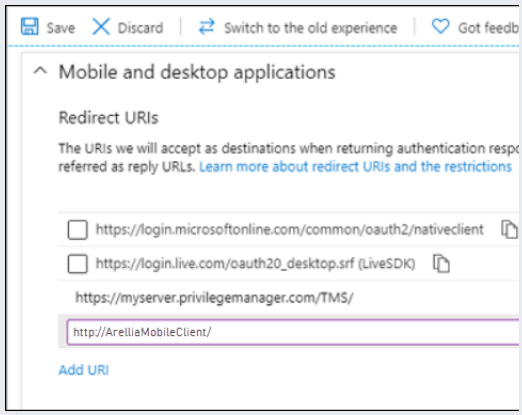
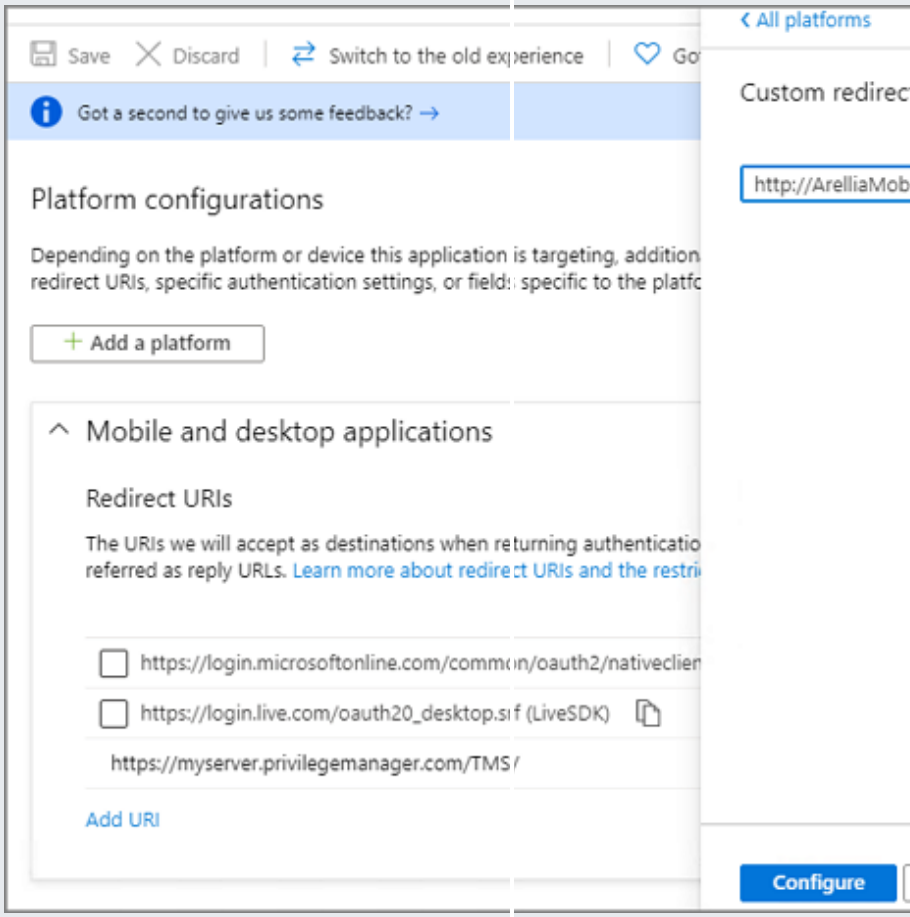
As a prerequisite for running the Privilege Manager Mobile Console, you must configure Azure Active Directory integration with Privilege Manager. Refer to Setting Up Azure Active Directory Integration in Privilege Manager.

Once Azure AD integration for your Privilege Manager instance is configured, follow these steps to add an additional Redirect URI for the mobile application to the Azure AD application registration:

1. Open the **Azure Management Console**.
2. Navigate to your **Active Directory** instance.

3. Select **App registrations** from the menu.
4. Click the **Owned applications** tab.
5. From the list under **Display name** select your Privilege Manager registration.
6. Either select the **Redirect URI** links or the **Authentication** menu.
7. Select **Add a platform**.
8. Select **Mobile and desktop applications**.
9. Set the Redirect URI to exactly `http://ArelliaMobileClient/`. There are two access points to do this either via:
   - Redirect URI or
   - Authentication menu.

   The following table shows the steps you will see for each option:

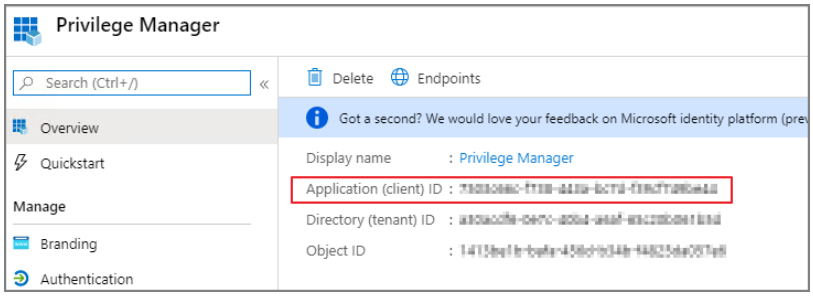
accessed via Redirect URI link	accessed via Authentication menu
	

accessed via Redirect URI link	accessed via Authentication menu
1. Click Add URI.	1. Enter `http://ArelliaMobileClient/`.
2. Enter `http://ArelliaMobileClient/`.	2. Click **Configure**.

Important: The URI value needs to exactly match `http://ArelliaMobileClient/`.

10. Click **Save**.

On the **App registrations** page under **Owned applications**, take note of the **Application (client) ID**. You will need to use the client ID when you Configure the Mobile Console in Privilege Manager.



Install and Configure the Mobile Console in Privilege Manager

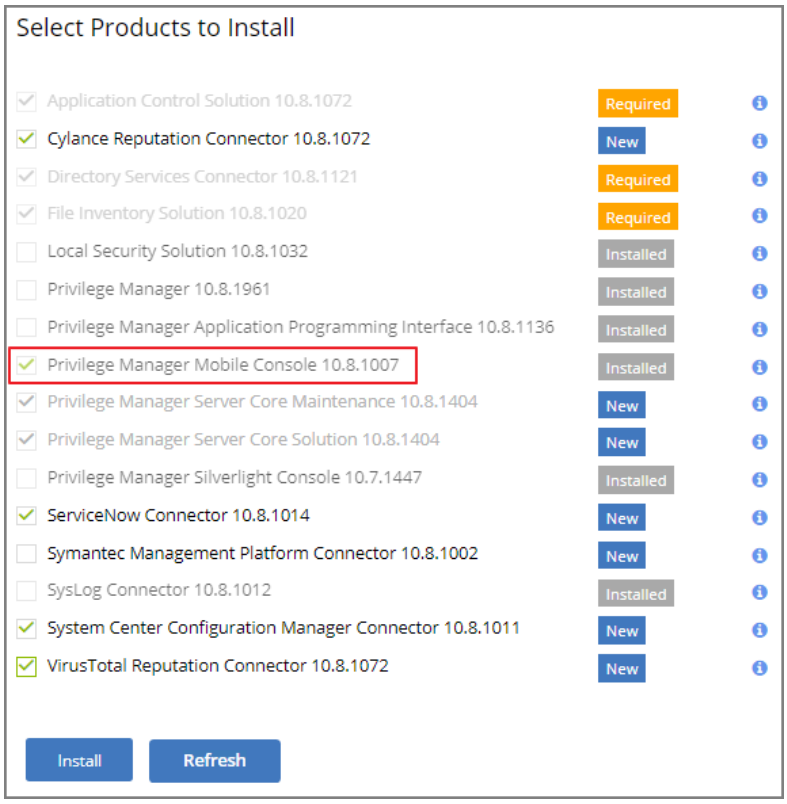
To configure the Mobile Console in Privilege Manager, you must:

1. Install the Privilege Manager Mobile Console.
2. Set the Client ID and Tenant ID.
3. Configure the notification settings.

Install the Privilege Manager Mobile Console

The Privilege Manager Mobile Console needs to be installed on the same server that is running the Privilege Manager instance.

1. Navigate to your Privilege Manager setup page or select **ADMIN | More...** and select the **Add / Update Program Features**.
2. Click **Select Products to Install**.



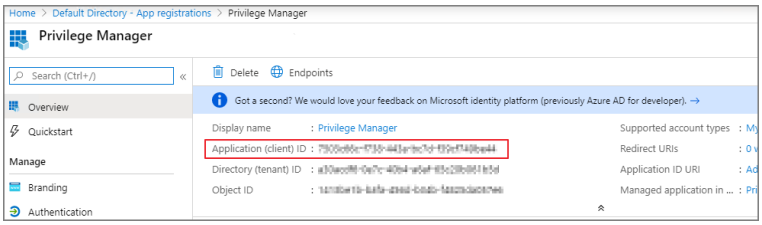
3. Select **Privilege Manager Mobile Console** and click **Install**.

Once the installation completes click **Home** to navigate back.

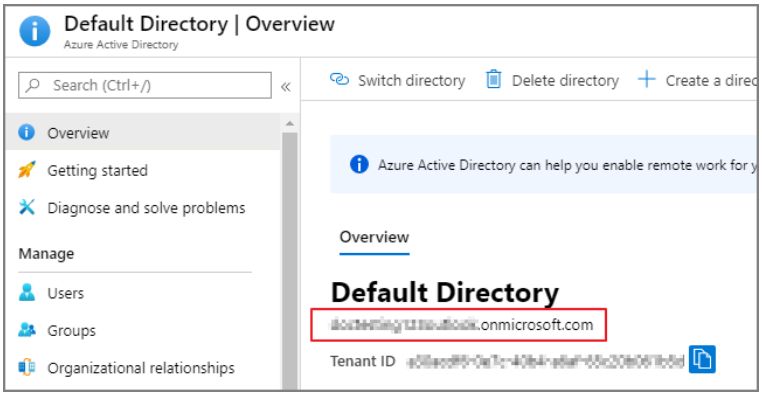
Set the Client ID and Tenant ID

After you have installed the Privilege Manager Mobile Console, set the Client ID and Tenant ID.

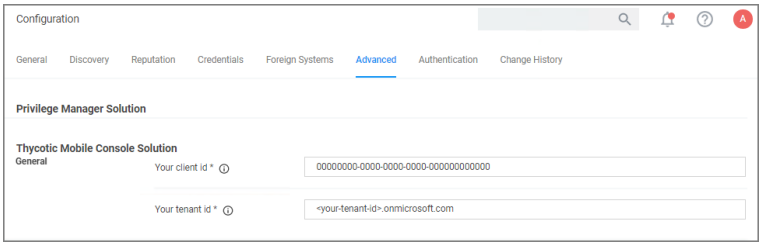
1. Navigate to **Admin | Configuration**.
2. Select the **Advanced** tab.
3. Scroll down and under **Thycotic Mobile Console Solution** under General enter values for:
   a. **Your client id**: In the **Your client id** field, enter the Client Id that you generated when you configured the Microsoft Azure Active Directory. In the Azure AD portal, you find this under App Registration. Look for the **Application (client) ID** value.



b. **Your tenant id**, is the DNS name of the Azure Active Directory instance. You find it on the Azure AD Home page, between the friendly name and the Azure Tenant ID, for example **name.myinstance.com** or **MyCompanyName.onmicrosoft.com**.



Enter that DNS in the **Your tenant id** field.

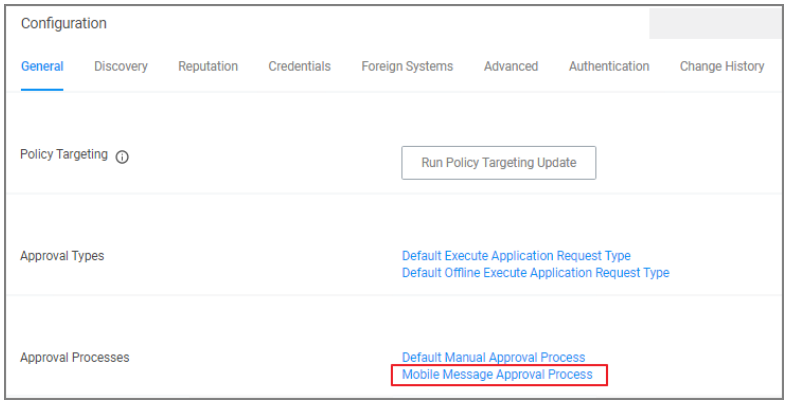


4. Click **Save Changes**.

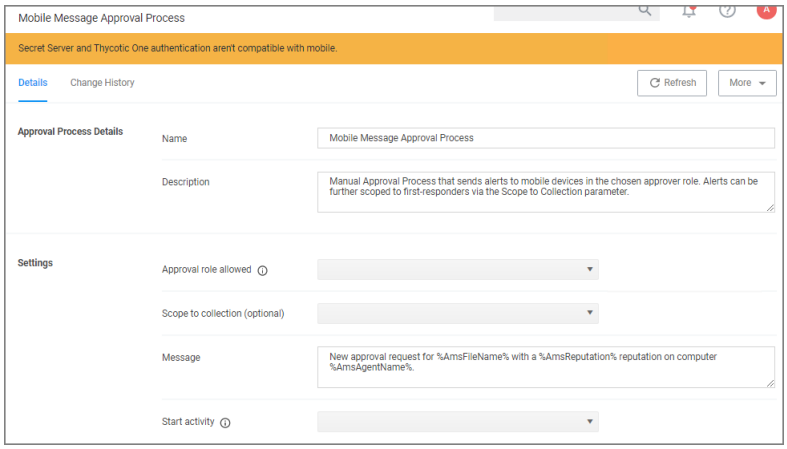
Configure the Notification Settings

The notification settings for the mobile app are available via general configuration and task automation.

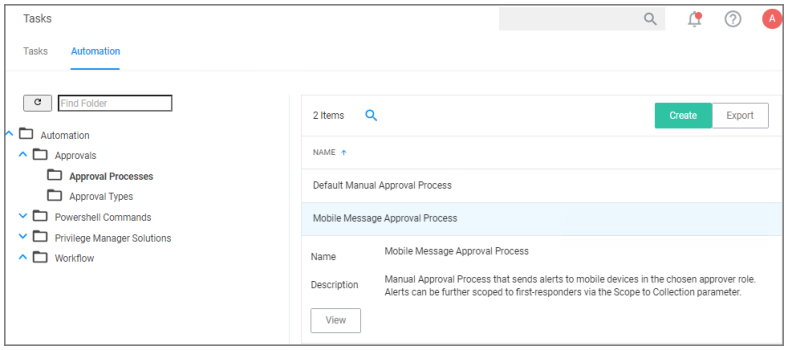
1. Navigate to **Admin | Configuration**.
2. Select the **General** tab.



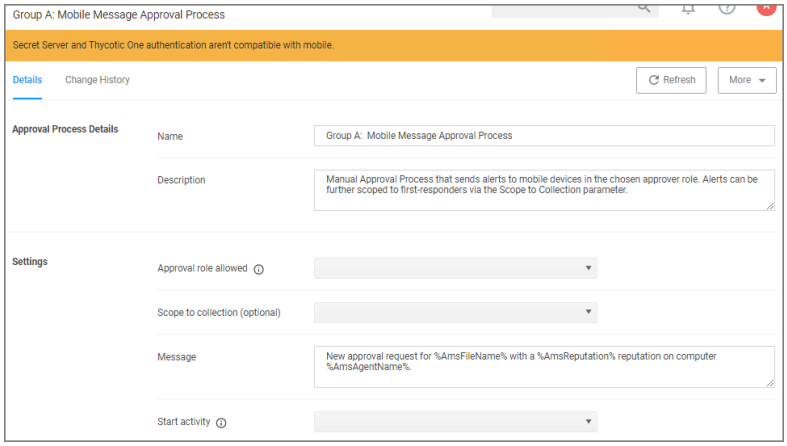
3. Under Approval Processes click **Mobile Message Approval Process**.



This task can also be accessed via **Admin | Tasks**, selecting the **Automation** tab and the in the folder tree **Automation | Approvals | Approval Processes | Mobile Message Approval Process**.



4. For customization, duplicate the default task. Give it a meaningful name for your environment.
5. Click **Create**.



6. Under **Settings**, you specify

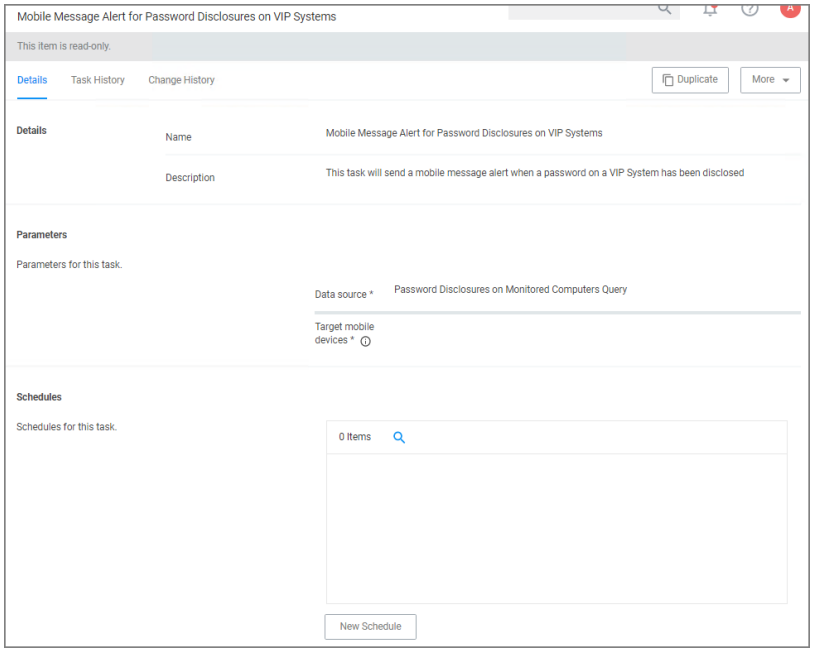
- **Approval role allowed**, which roles have approval permissions. By default the alerts for new approval requests will only be sent to mobile users in the Administrators role. You can change this setting by adding the approver role to a different role.
- **Scope to collection (optional)**, which is an optional setting, to scope these messages to a subset of users in that role.
- **Message**, what message will be displayed to the approver when a approval request was triggered.
- **Start activity**, which is an optional setting, any activity you wish to start as part of the approval.

7. Click **Save Changes**.

To start sending notifications to phones, select the **Default Execute Application Request Type** and change the **Approval Process** from the **Default Manual Approval Process** to the **Mobile Message Approval Process** and save the changes.

> **Note:** The approval process change to Mobile Message Approval Process is only for the notification message that an approval was requested. The actual approval has to be followed through via HelpDesk interface. Currently approval requests cannot be approved via the Mobile app.

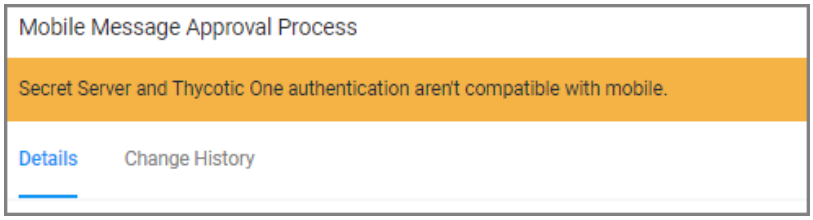
You can also send notifications based upon report data. These can be used to send alerts for suspicious activity, etc. An example of this can be found under **Tasks | Server Tasks | Mobile Messaging | Mobile Message Alert for Password Disclosures on VIP Systems**.



This message can be executed on a schedule to send alerts for any password disclosures on VIP Systems. VIP Systems are configured via the Monitored Computers parameter that allows you to choose a Collection of computers.

Authentication Provider Warning

The Privilege Manager Mobile Console does currently not work with Secret Server or Thycotic One as the authentication provider. If Secret Server is configured as the authentication provider in Privilege Manager, a warning message is shown on the Mobile Message Approval Process configuration page.



Configure the Service Bus for Mobile

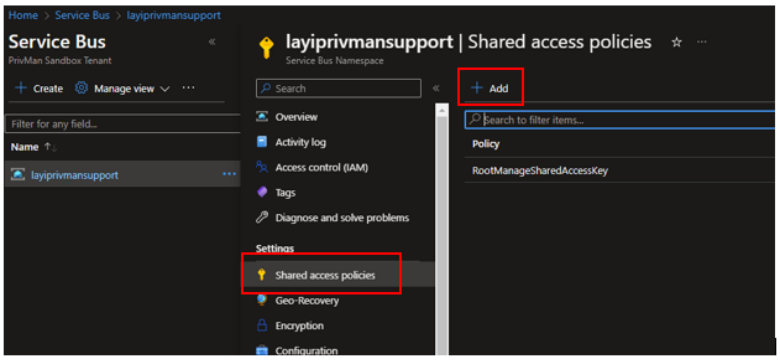
Creating a Service Bus and Queue in the Azure Portal

When a Service Bus Queue needs to be created, refer to the latest instructions as outlined by Microsoft in Quickstart: Use Azure portal to create a Service Bus queue.

If you already have an existing Service Bus in Azure, you are welcome to use the existing setup. You just need to create a new queue within your existing Service Bus to be used by the Mobile App.

The following steps explain what is required for the Mobile App integration:

1. In the Azure Service Bus portal go to the **Shared access policies** page.
2. Find the policy called **RootManageSharedAccessKey**. If you don't have one yet, create one by that name and select the **Manage** option and save it.
3. On the **RootManageSharedAccessKey** policy you can see the **Primary Key** field. Make note of where this is. We have to use it in a step down below.
4. Next, navigate to the **Queues** page and create a new queue.
5. Create a new Shared Access policy names **RootManageSharedAccessKey** for the new queue.



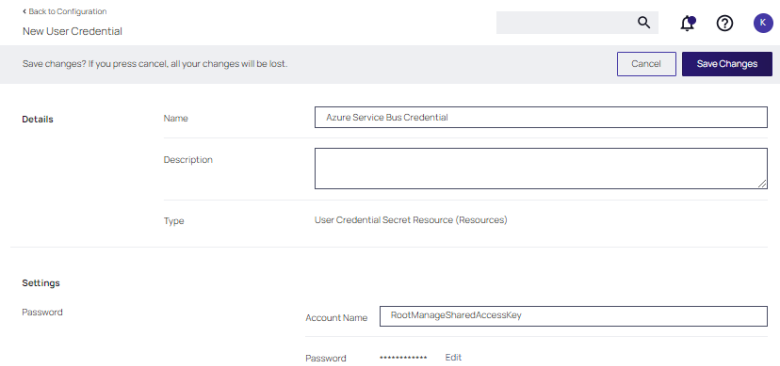
6. Do not check any of the options, using the defaults is fine. Take note of the name of the newly created queue.

Next you will need to follow the instructions below to create a credential for the Service Bus and add the Service Bus as a foreign system in Privilege Manager.

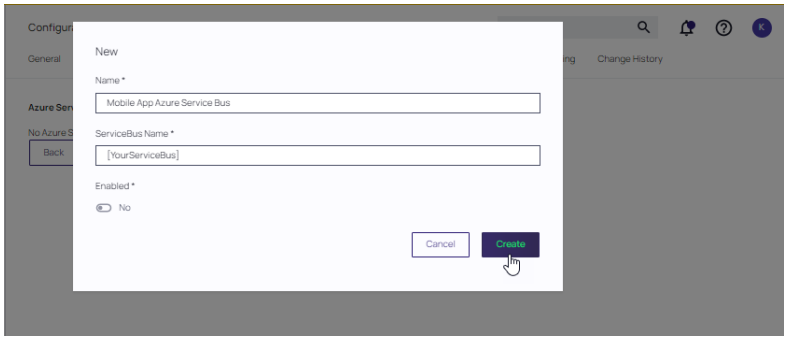
Adding the Service Bus as a Foreign System

The Azure Service Bus requires a Foreign Systems configuration in Privilege Manager. To configure a Service Bus instance with a custom URL and credentials follow these steps:

1. In the Delinea Privilege Manager Console, click **Admin | Configuration**.
2. Click the **Credentials** tab.
3. Click **Create**.
   - Enter a **Name**, for example *Azure Service Bus Credential*.
   - Set the Account name to **RootManageSharedAccessKey**.
   - Set the Password to the value of the **Primary Key** obtained during the Azure Service Bus configuration procedure **step 3** under "Creating a Service Bus and Queue in the Azure Portal" above.
4. Click **Save Changes**.



5. Navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
6. Click the **Azure Service Bus** option.
7. Click **Create** at the prompt box for creating a new service bus.

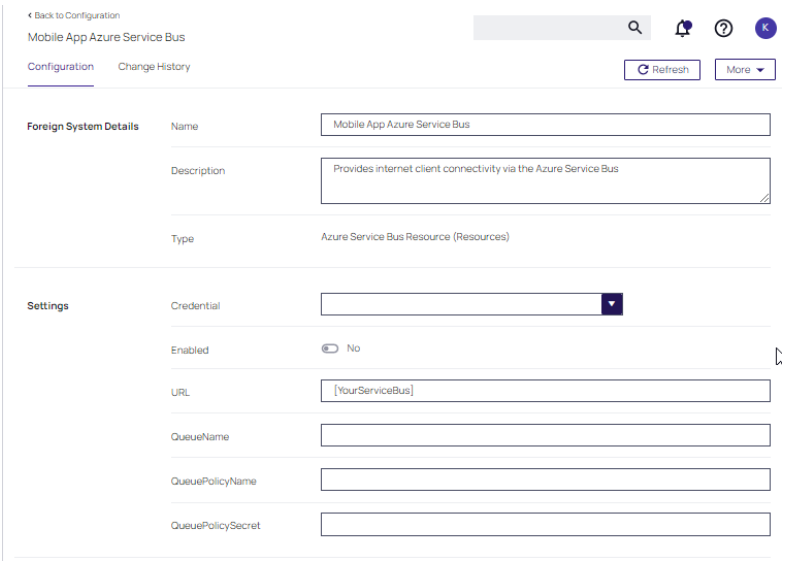


   - Enter a **Name**, for example *Mobile App Azure Service Bus*.
   - Set the **ServiceBus Name** to the namespace of the Service Bus from the Azure Portal. To find this value, open the Azure Portal, locate the Service Bus that is being used for this integration (refer to the intro above).

Go to the **Properties** page and locate the Name property (generally, this is the same name as the instance you just located in the list of Service Bus instances).

- Set the **Enabled** switch to **No** for now.

8. Click **Create**.
9. Enter the requested information at the Mobile App Azure Service Bus configuration page.
   - Set the credential to the credential created in step 3 of this procedure (*Azure Service Bus Credential*).
   - Leave the URL field as is (and ignore the fact that it's called URL - it's just the Service Bus name).
   - Make sure the URI matches the first part of the namespace created in Azure.
   - Set the QueueName to the same queue name created above in **step 4** under "Creating a Service Bus and Queue in the Azure Portal".
   - Set the Queue Policy Name to **RootManageSharedAccessKey**.
   - Set the Queue Policy Secret to the **Primary Key** as obtained in **step 5** under "Creating a Service Bus and Queue in the Azure Portal" above.
10. Click **Save Changes**.



11. Enable the Service Bus and toggle **Enabled** to **Yes**.
12. To verify everything is working correctly, open your browser and point it to the ServiceBus worker service:
    - **On-Premises**: `https://yourinstance.privilegemanager.com/Tms/ServiceBus/WorkerService.svc`
    - **Cloud**: `https://yourinstance.privilegemanagercloud.com/Tms/ServiceBus/WorkerService.svc`

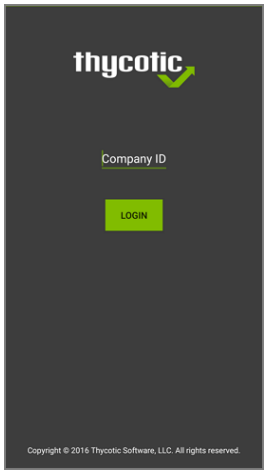
    Wait for the page to respond. See example below. You are now ready to install the Delinea ACS application on your mobile devices.

Note:
If the page does not respond, try the URL again in a few minutes. If the error persists, perform the recommended [Troubleshooting](troubleshooting-bus.md).

Mobile App Install and Sign In

After installing and configuring the server components, help desk users can download the Mobile app for their smartphone via the appropriate app store by searching for **Thycotic ACS**. After you install the app, do the following:

1. Open the application on the mobile device.



2. When prompted for the **Company ID**, enter the name of your **Service Bus**. To find the name, open the Azure Portal, locate the Service Bus that is being used for this integration. Go to the **Properties** page and locate the Name property (generally, this is the same name as the instance in the list of Service Bus instances).
3. Next enter the Azure Active Directory user credentials.
4. Create a pin to secure the Mobile app.

Troubleshooting

If you experience any issues completing those steps, try the following to solve the problem:

1. Verify that you can reach the Service Bus worker service by pointing your browser at the ServiceBus worker service. Enter the URL into your browser navigation bar:
   - **On-Premises**: `https://yourinstance.privilegemanager.com/Tms/ServiceBus/WorkerService.svc`
   - **Cloud**: `https://yourinstance.privilegemanagercloud.com/Tms/ServiceBus/WorkerService.svc`

   Wait for the page to respond.
2. Verify the Redirect URI setting in your Azure AD application registration matches the configuration values in Privilege Manager.
3. **Recycle the App Pools on the Privilege Manager Instance** following any changes for this integration. Without the recycle, the new settings won't be applied.

   Cloud customers, please contact support for assistance to get these recycled. Unfortunately, this is a "must-contact" situation.

Troubleshooting the Mobile Application

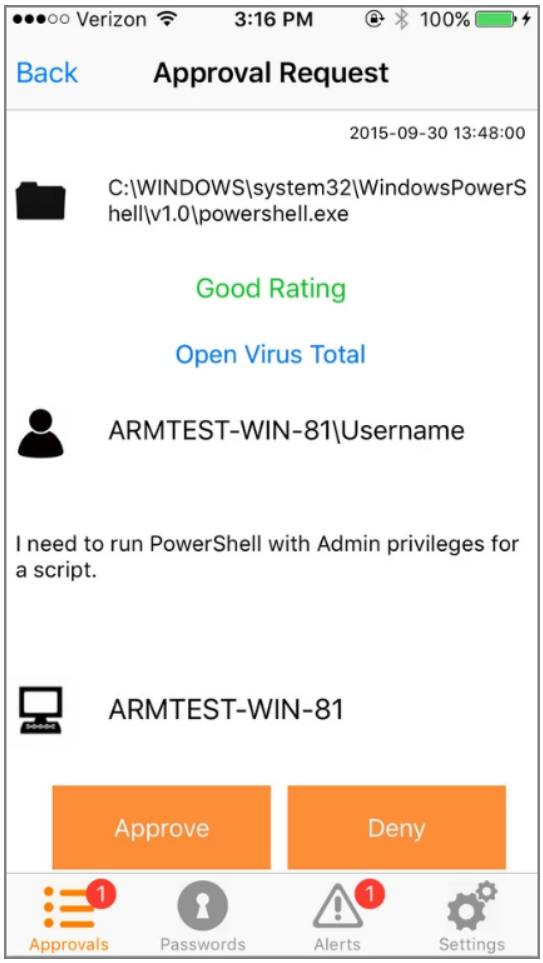
In the event that you receive an error message and were not successful in receiving a response from the On Premise or Cloud Service Bus page, perform the following troubleshooting steps:

- Verify the ServiceBus worker service has started (on premise or cloud).
  - **On-Premises**: `https://yourinstance.privilegemanager.com/Tms/ServiceBus/WorkerService.svc`
  - **Cloud**: `https://yourinstance.privilegemanagercloud.com/Tms/ServiceBus/WorkerService.svc`
- Ensure that the correct **RootManageSharedAccessKey** is assigned to the correct queues for both the Service Bus and second queue associated with the Service Bus. Refer to Creating a Service Bus and Queue in the Azure Portal.

Use the Mobile Application

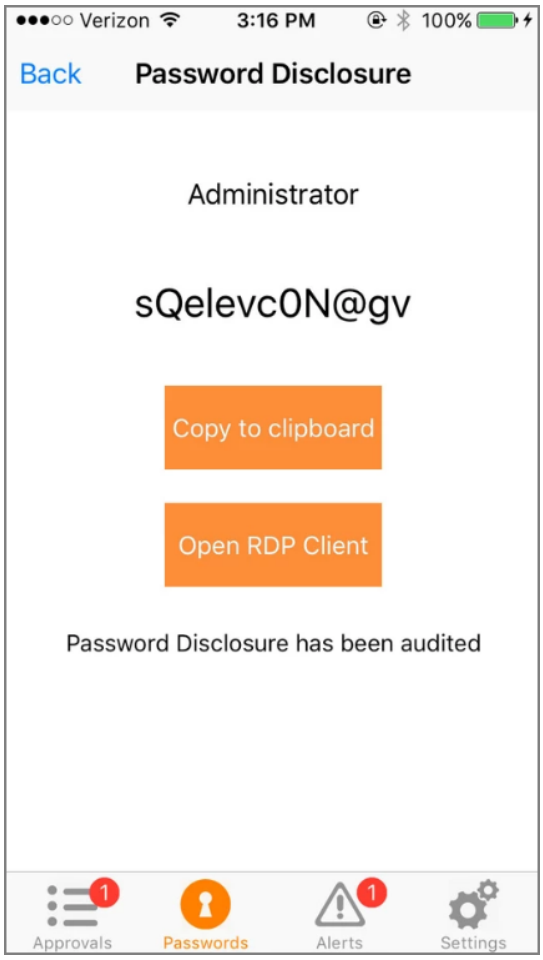
Approval requests

Approval Requests area provides the ability to approve/deny pending approval requests and the ability to view recently approved requests.



Password Disclosure

Password Disclosure area provides the ability to disclose managed user passwords that the mobile user has access to.



Alerts

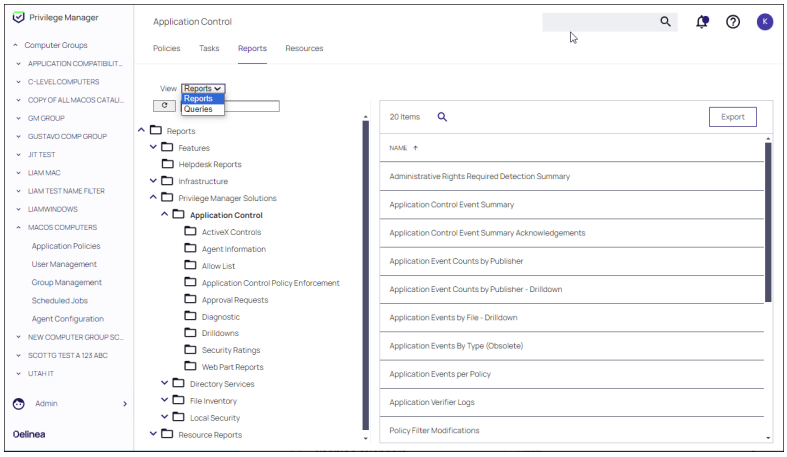
The Alerts area provides the ability to view non-approval request alerts, such as the Password Disclosures on VIP Systems. These alerts can be forwarded via email or removed.

Reports

Privilege Manager includes an array of reports. All reports are accessed from the Reports and Queries page.

1. Navigate to Admin | Folders.
2. Click the Reports tab.
3. Select Reports or Queries at the drop-down to view the associated content.

4. Select any report, then click **View** for its details.



Out-of-the-Box Reports

To access a list of relevant out-of-the-box reports that span a spectrum of system activity and diagnostic information in Privilege Manager, select **Reports** from the left navigation panel.

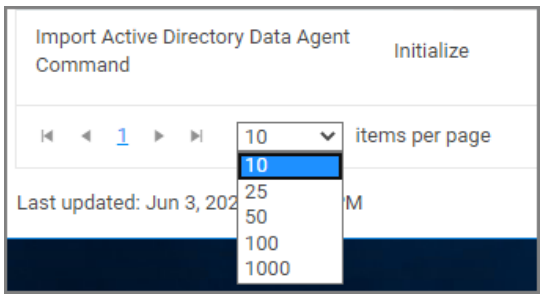
Refer to "Out-of-the-Box Reports" on the next page.

Commonly Used Reports

For ease of use, some of the more commonly used reports are displayed in this documentation table of content. Click any link for more information regarding these reports.

Data Records Displayed

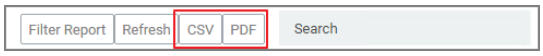
Users can adjust the amount of data entries to display per page. When you adjust this number of rows on a page



The default number of data grid rows to display on pages across the Privilege Manager UI is set via "Navigation and Controls" on page 13.

Export Options

Privilege Manager reports can be exported via **CSV** and **PDF** export option buttons.



Once the **CSV** or **PDF** button is clicked, users can choose to:

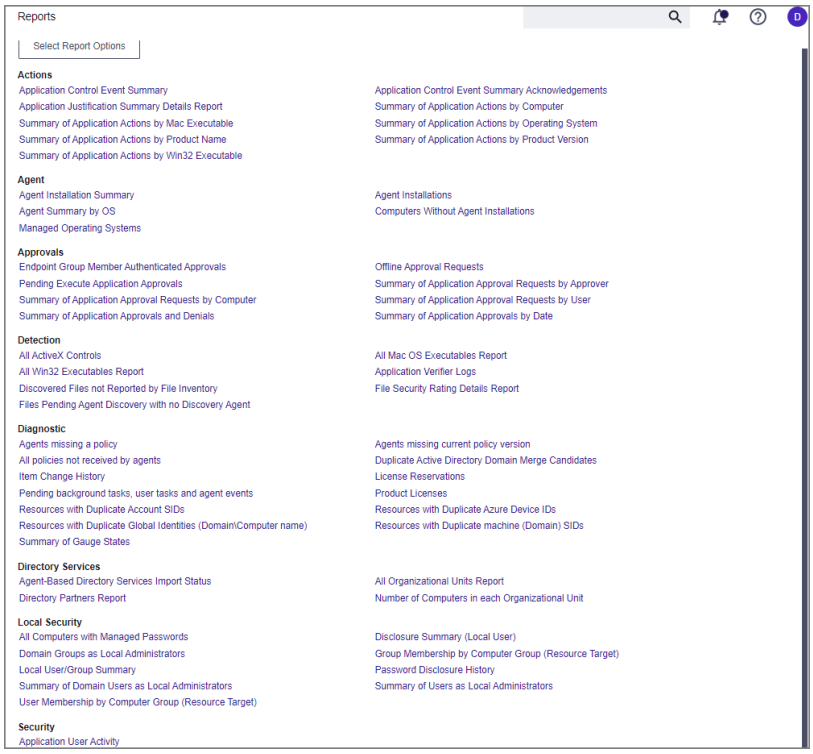
- export the current page or
- export all pages.

Note: Selecting all pages might take some time to complete, depending on the overall size of the data records to export.

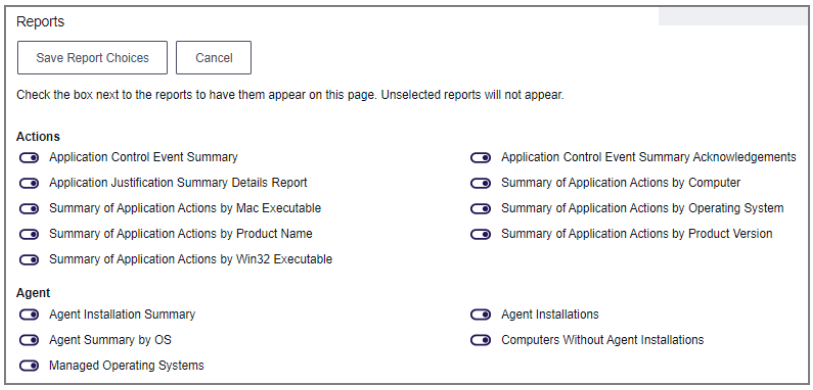
Out-of-the-Box Reports

To access a list of relevant out-of-the-box reports that span a spectrum of system activity and diagnostic information in Privilege Manager, select **Reports** from the left navigation panel.

Click on the name of any of these reports to access details about your system.



The **Select Report Options** button lets users customize which of the default report options are shown on the Reports landing page.



By default all reports are listed on the Reports landing page. Use the switch to disable showing any given report.

Commonly Used Reports

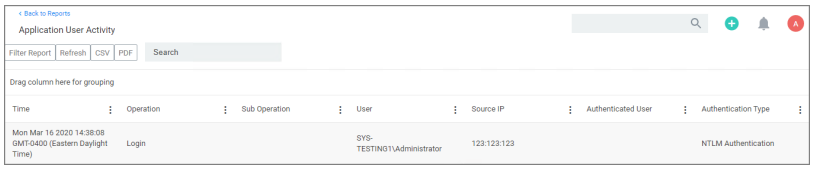
The following commonly used reports are provided for use.

- "Application User Activity" below
- "Membership by Computer Group Reports" on the next page
- "Change History Report" on page 889
- "Domain Users in Administrator Group" on page 890
- "Duplicate Active Directory Domain Merge Candidates" on page 891
- "Duplicate Resource Reports" on page 891
- "Logon Session Summary Report" on page 892
- "Performance Reporting" on page 893
- "Primary User" on page 898
- "Product Licenses" on page 900
- "Policy Modifications Reports" on page 895
- "Reports and Queries" on page 900

Application User Activity

Auditing for user activities like logins and logouts can be viewed via the Application User Activity report. The report is a chronological data collection of user login/logout events and relating data.

To access the report navigate to **Reports** and locate the **Security** reports, select **Application User Activity**.



User activity auditing is by default enabled. The following auditing data is stored and provided via report:

- User resource ID.
- Username associated with the resource ID.
- IP address from the system used to login.
- Date and time of the login/logout.
- Activity information, like successful login, unsuccessful login, logout, etc.

The report can be distributed via standard Email Report task.

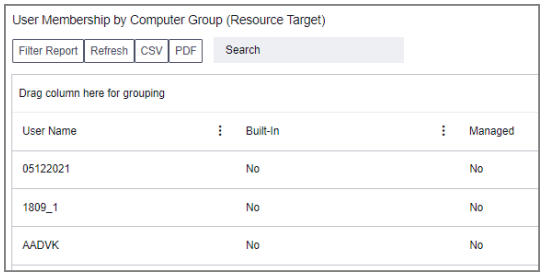
Membership by Computer Group Reports

Two reports are available to report on User and Group Memberships by Computer Group (Resource Target).

User Membership by Computer Group (Resource Target)

The User Membership by Computer Group (Resource Target) report lists all User Names that are part of a configured computer group. The table columns can be customized and sorted for grouping purposes.

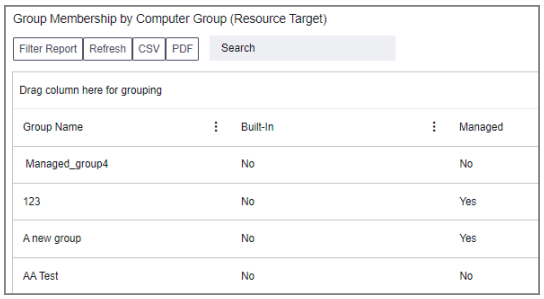
Default columns are User Name, Built-in, Managed, and Inventoried.



Group Membership by Computer Group (Resource Target)

The Group Membership by Computer Group (Resource Target) report lists all groups that are part of a configured computer group. The table columns can be customized and sorted for grouping purposes.

Default columns are Group Name, Built-in, Managed, and Inventoried.



Change History Report

Administrators need to be able to look at changes done by other users in Privilege Manager. The need to be able to audit any issue causing changes to configuration settings, policies, filters, and actions. The new **Change History Report** allows Privilege Manager Administrators to track changes and their impact on endpoints.

As part of the audit the following information is recorded:

- User account initiating the change.
- Date/Time of the change.
- Description of the change made.

The following changes are reported:

- Configuration settings to Advanced, Discovery, and Reputation items (new tab on Configuration page)
- Changes to items, like
  - User and Group changes inside Roles
  - Credentials added or existing credentials updated
  - Foreign system added or existing updated
  - Any setting in the Advanced tab
  - Changes to conditions of user editable resources.
- Policy, actions, filters, resource target changes, and additions (new tab on policy, actions, filters, resource target pages)
- Editing of task schedules (parameters and schedule of a task) - any change made to the schedule and parameters (New tab on task schedule page for each individual task)
- Imports and Saves of XML - differentiate between import and save

The reporting of any of these changes cannot be turned off and the results can be filtered by categories like Policy, Filter, Action, and Configuration.

Each save creates or adds to the revision history of items. The **Item Change History Report** cannot be used to revert to a previous state.

Item Change History

Filter Report | Refresh | CSV | PDF | Search

Drag column here for grouping

Name	Operation	User	Date	Correlation ID
New User Credential	CreateFromTemplate	\Administrator	7/7/2020 9:10 AM	ed74b28d-399d-4a79-9141-3e691122b2a8
Create inbound TCP firewall rule for Elevate Adding Inbound TCP Firewall Rule Privilege	CreateFromTemplate	\Administrator	7/6/2020 11:00 PM	368940d4-94d9-4cee-8a8f-971f1808882c
New Display Advanced User Message Action (MacOS)	Save	\Administrator	7/6/2020 9:00 PM	3ca93080-bfa0-4e02-8cfa-277e2fd6bab6
New Display Advanced User Message Action (MacOS)	CreateFromTemplate	\Administrator	7/6/2020 9:00 PM	6e1841e1-f2af-4c4d-af1f-6ee089e3088b
Test of Application Denied Notification Action	Clone	\Administrator	7/6/2020 8:24 PM	f96f463e-1c58-4058-b10f-2c81f3b24f09
Copy of Deny Execute Message	Clone	\Administrator	7/6/2020 8:07 PM	2b3ecc9f-5e52-4644-a488-854a07c1682b
New Adjust Process Rights Action	Save	\Administrator	7/6/2020 7:42 PM	c9675353-5e6e-4185-8e8f-18f9faf2956b
New Adjust Process Rights Action	CreateFromTemplate	\Administrator	7/6/2020 7:42 PM	c73da2d0-8fe5-4001-bae9-7ebe7c42b9d8
New Set Process Security Descriptor	Save	\Administrator	7/6/2020 7:24 PM	ec86ef31-4dfd-4692-b2dd-3aa633d69f84
New Set Process Security Descriptor	CreateFromTemplate	\Administrator	7/6/2020 7:24 PM	1b41a4cc-1651-4089-ab16-446c7b133ab4

Domain Users in Administrator Group

You can get instant reports by clicking the **Reports** tab. To see which domain users are members of the administrators group, view the domain users as local administrators report.

Local Security

- All Computers with Managed Passwords
- Domain Groups as Local Administrators
- Password Disclosure History
- Summary of Users as Local Administrators
- Disclosure Summary (Local User)
- Local User/Group Summary
- Summary of Domain Users as Local Administrators

Click the **Summary of Domain Users as Local Administrators** report to view details:

Reports › Summary of Domain Users as Local Administrators

Filter Report | Refresh | CSV | PDF | Search

Drag column here for grouping

Builtin	Account Type	Group Name	User Name	Computers
User Defined	Domain	administrators		1
User Defined	Domain	domain admins		1
User Defined	Domain	domain admins		1
User Defined	Domain	domain admins		1
User Defined	Domain	domain admins		1
User Defined	Domain	domain admins		1
User Defined	Domain	domain admins		1
User Defined	Domain	domain admins		1
User Defined	Domain	domain admins		1
User Defined	Domain	domain admins		1

Selecting any of the accounts listed, open the Drilldown report for that specific item:

Reports › Summary of Users as Local Administrators - Drilldown

Filter Report | Refresh | CSV | PDF | Search

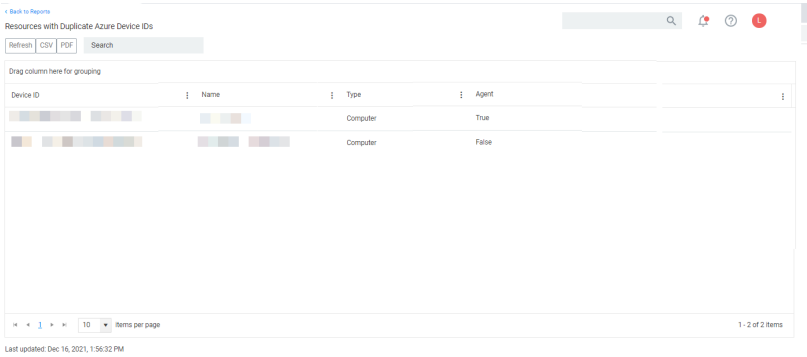
Drag column here for grouping

Computer Domain	Computer	Builtin	Account Type	Domain	Group Name	User Name
name.yourdomain.com	GO-TEST-SYS	User Defined	Domain	TESTENV	domain admins	anotheradmin

Duplicate Active Directory Domain Merge Candidates

This report identifies any existing Active Directory Domains that have been duplicated. Refer to the new Merge Duplicate Active Directory Domains task to address these duplicates.

To view this report, locate the Diagnostic section of the Reports page. Select **Duplicate Active Directory Domain Merge Candidates**. If desired, drag-and-drop the report headers to modify the sort hierarchy. Columns can also be sorted. Click **CSV** and **PDF** to export the report to the associated format.



Duplicate Resource Reports

Four reports are available to identify any duplicate Computers, Domain Users, and Domain Groups associated with your instance of Privilege Manager.

They can be accessed under the **Diagnostic** section of the Reports page.

Resources with Duplicate Account SIDs

This report will list Computers, Domain User, and Domain Groups associated with the Privilege Manager Server, that have identical Account SIDs.

Resources with Duplicate machine (Domain) SIDs

This report will list Computers associated with the Privilege Manager Server that have identical Domain SIDs.

Resources with Duplicate Azure Device IDs

This report will list Computers associated with the Privilege Manager Server that have identical Device IDs.

Resources with Duplicate Global Identities (Domain\Computer name)

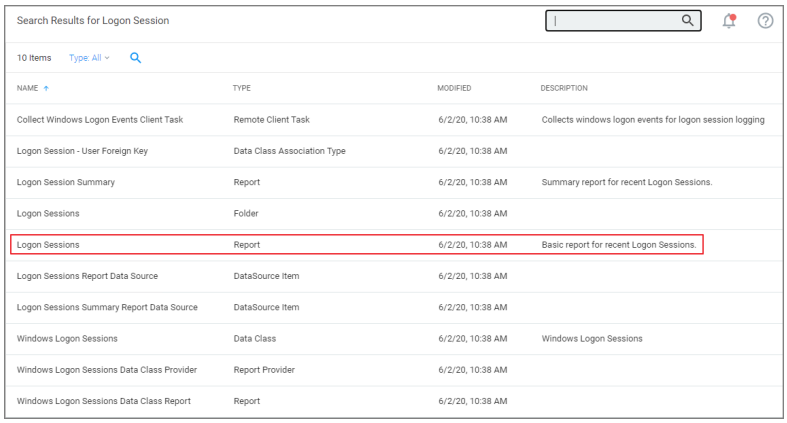
This report will list Computers, Domain User, and Domain Groups associated with the Privilege Manager Server, that have identical Account Names.

Note: Information regarding the tasks that are run to address the duplicates identified in these reports are found in Server Tasks. They are: **Merge Duplicate Active Directory Domain** and **Remove Active Directory Domain**.

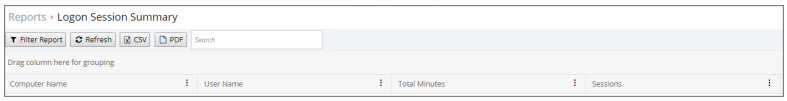
Logon Session Summary Report

The Summary report for recent Logon Sessions.

1. Navigate to the Privilege Manager Dashboard.
2. In the Search field enter **Logon session**.



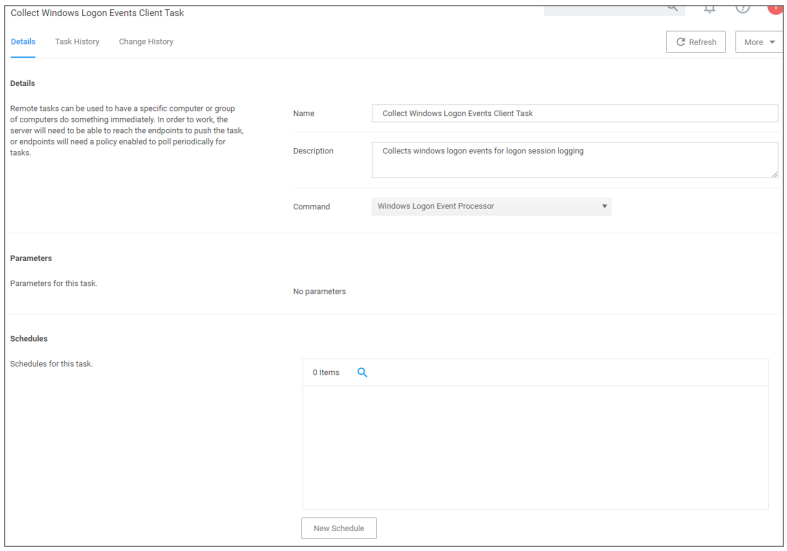
3. Click on **Logon Session Summary**.
4. The report contains the information for the Computer Name, User Name, total minutes and sessions.



Note: You can also run the **Collect Windows Logon Events Client Task** to get updated windows logon events for logon session logging.

Using the Collect Windows Logon Events Client Task

1. Navigate to **Admin | Tasks | Client Tasks** and select **Local Security**.
2. Click **Collect Windows Logon Events Client Task**.



3. Run the task.

Performance Reporting

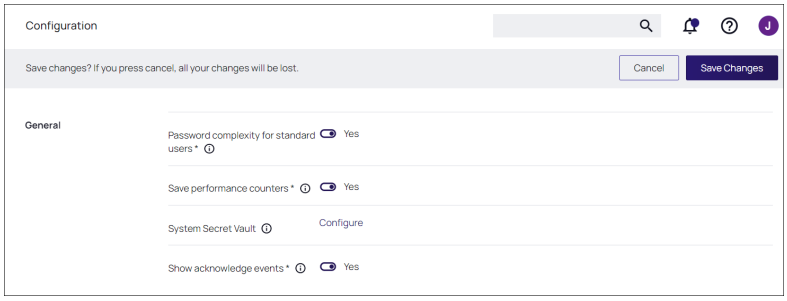
Performance Reporting, available for Privilege Manager 10.5 and later, keeps admins abreast of all activity across the network that could potentially impact Privilege Manager server performance.

Nightly tasks collect performance information via the following reports:

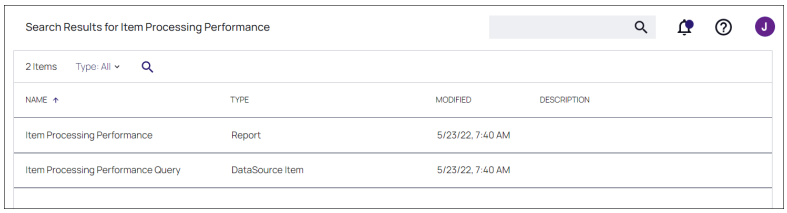
- Item Processing Performance
- Processing Performance

Setting up Performance Reporting

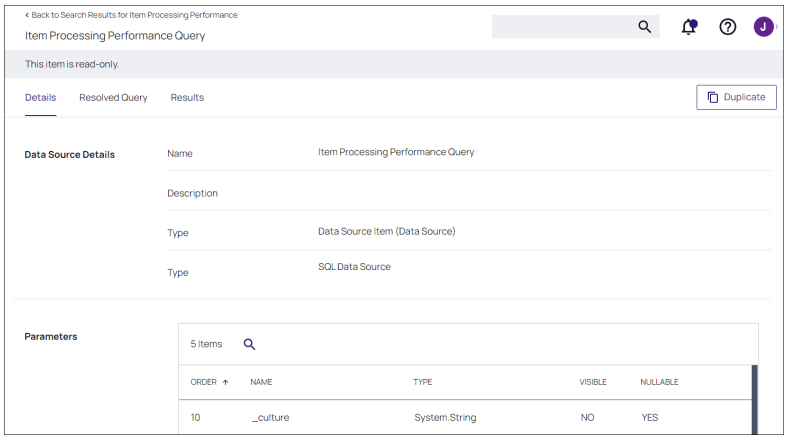
1. Navigate to **Admin** | **Configuration**.
2. Select the **Advanced** tab.
3. Scroll to the **General** section, activating **Save performance counters** by sliding the switch to the **Yes** position.



4. Click **Save Changes**.
5. Locate the performance reports by entering **Item Processing Performance** or **Processing Performance** in the search bar.



6. Select the report you want to view.



Tracking Agent Events

To enable customers to track agent events passed to the server, the **agentevent** category displays on the **Item Processing Performance** report. The report displays all applicable agent events that pass messages to the server. These include, but are not limited to, the following events:

Application Control

- Application Actions
- Justifications
- App Metering

Core

- Basic Inventory Events
- Discovery Events

File Inventory

- File Inventory
- File Location Inventory

Local Security

- Local User/Group Inventory
- User Logon Inventory

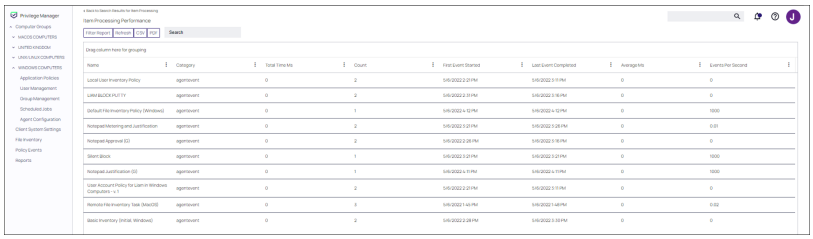
- Randomize Password
- COM Object Inventory
- Service Inventory

Directory Services

- Import Data Events

In the past, competing group membership policies could cause excessive uploads that impacted performance. Reviewing this report allows Privilege Manageradmins to both identify policies that may be causing issues and take corrective action, such as making policy scheduling adjustments.

The image below displays examples of policy events that have been passed to the server.



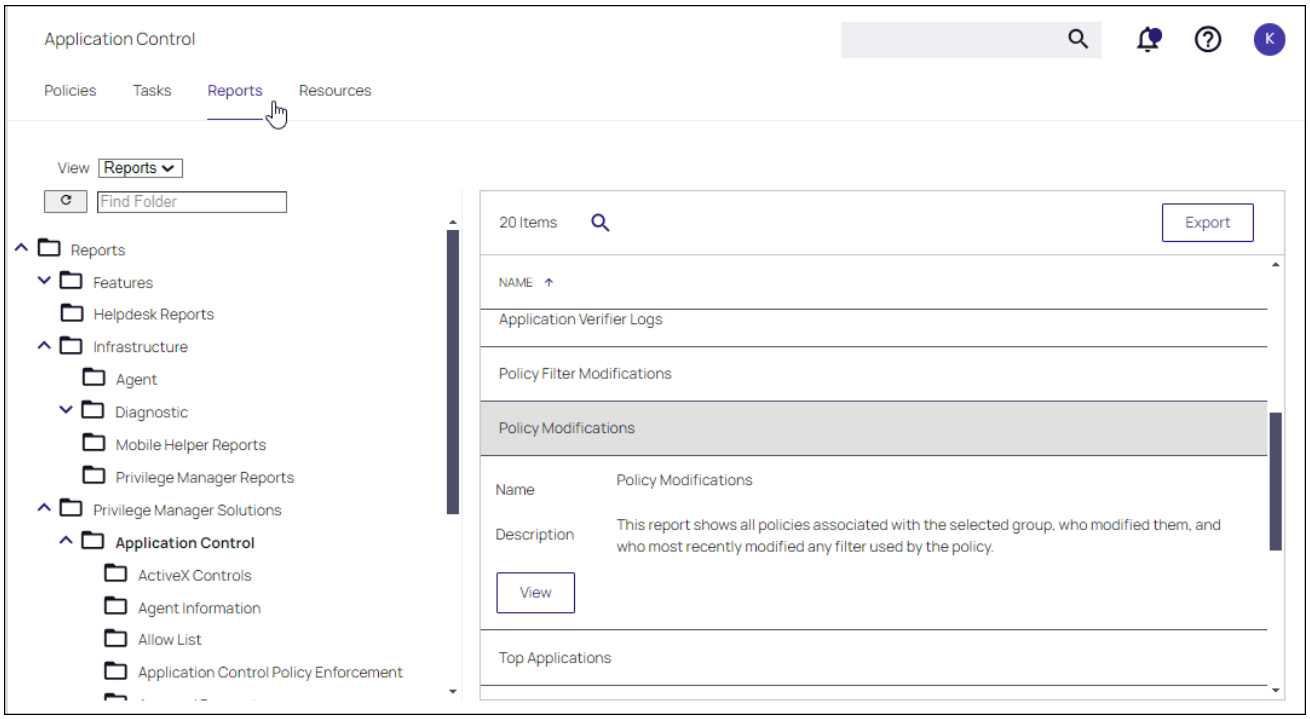
Policy Modifications Reports

Two reports, available in Application Control, provide details of the policies and policy filters configured in a Computer Group.

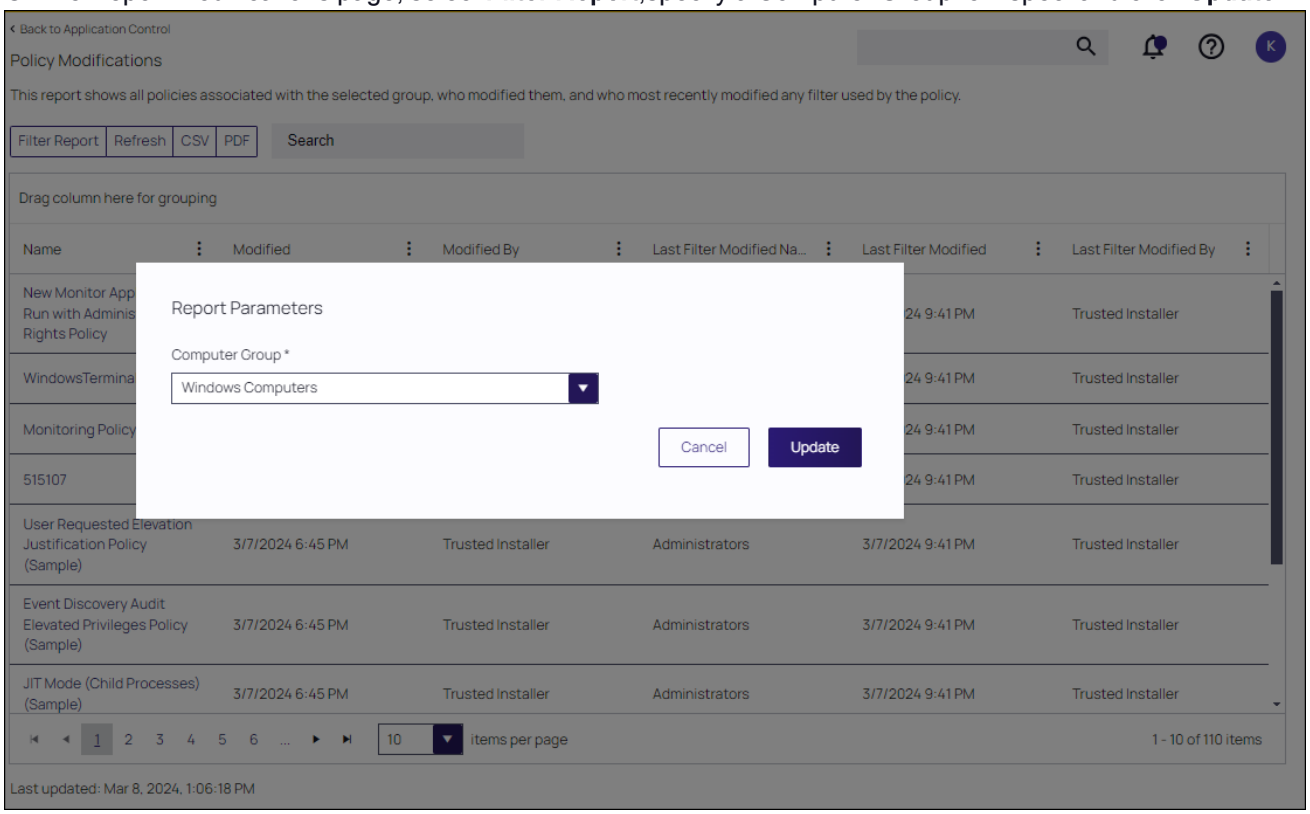
- A top-level report, Policy Modifications, shows all policies in a group, when they were modified, and also the most recently modified filter in that policy.
- A Policy Filters Modifications report drills down into a Policy Modifications report to show updates to filters.

Viewing a Policy Modifications Report

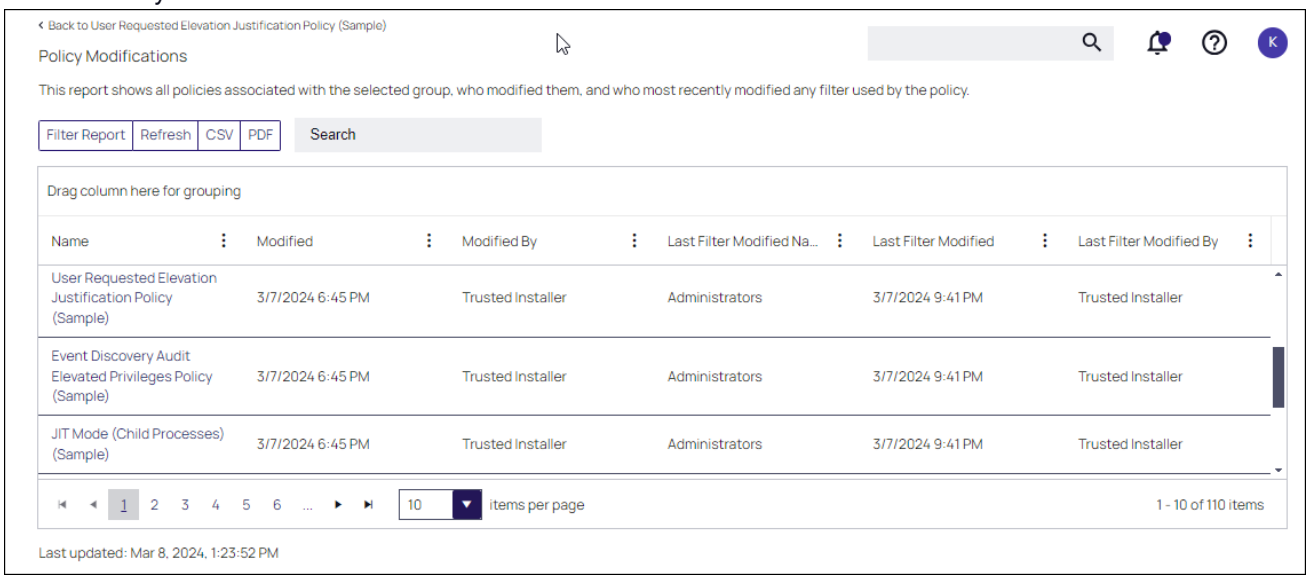
1. Select **Admin** | **Folders**. On the Reports page, select the **Reports** tab.
2. Open the Reports tree and navigate to **Privilege Manger Solutions** | **Application Control**.
3. Locate the Policy Modification report in the reports listing. Select the report and click **View** to view the report details.



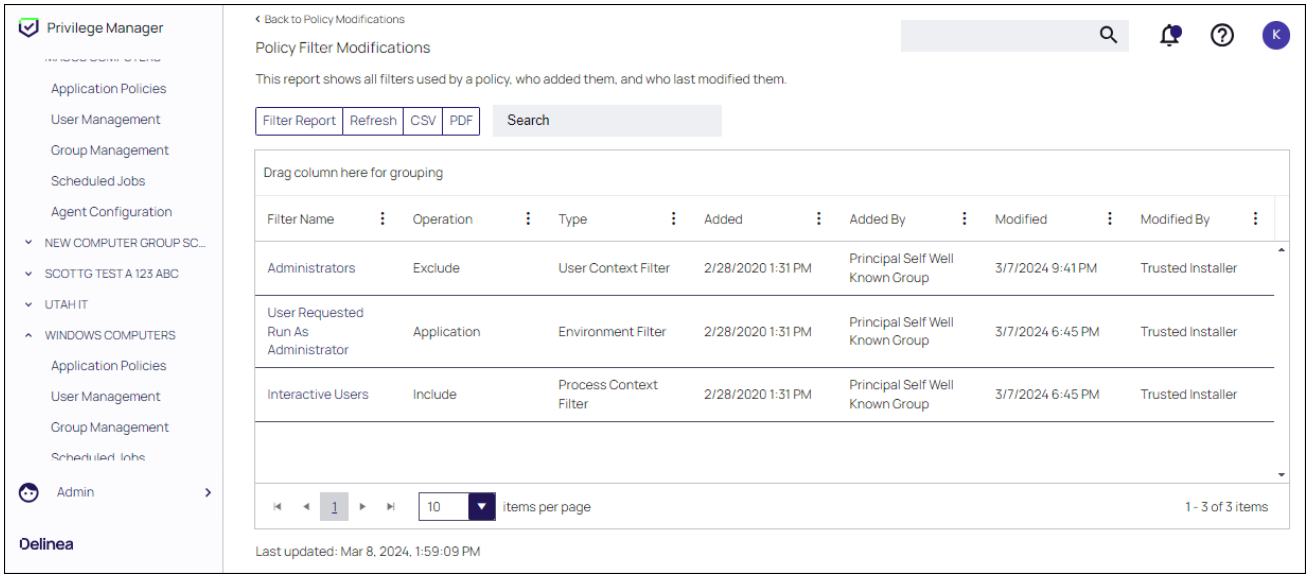
4. On the Report Modifications page, select **Filter Report**,specify a Computer Group to inspect and click **Update**.



5. The details displayed include the policies in that Computer Group. Select a policy to view the associated policies and when any filters were modified.



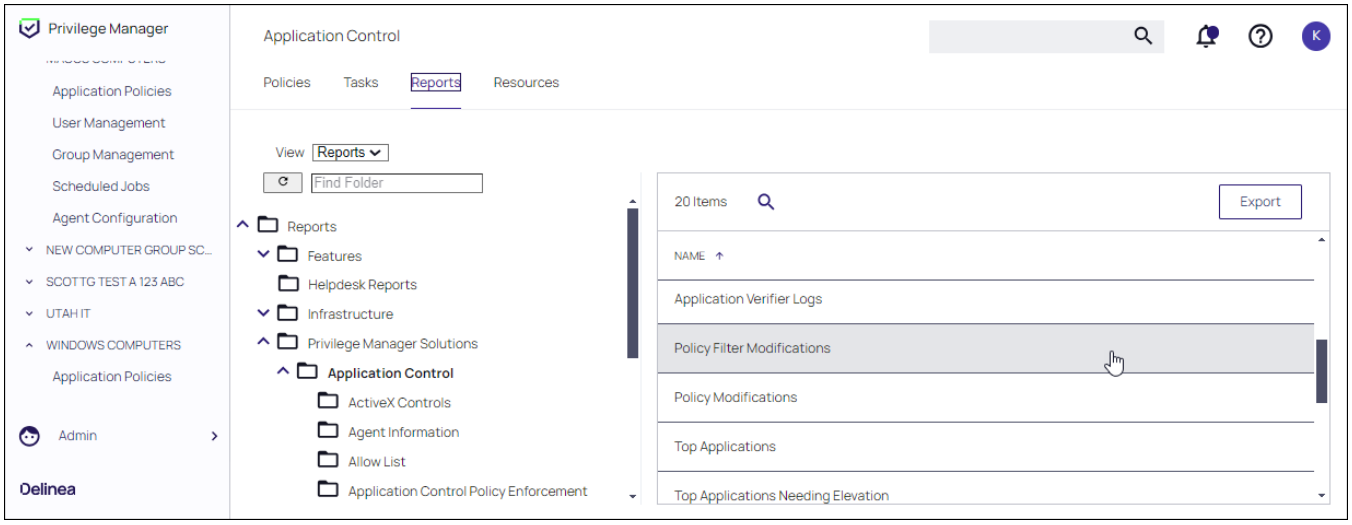
6. Select any filter to view the Policy Filter Modification page.
7. These details include the filter operation associated with the policy, the type of filter, when it was added or added to its parent and when the filter was modified.
8. Select any filter to view its details.
9. Select **Back to Policy Modification** at the top of the page to return to the Policy Modification page and select another policy for review.



Viewing a Policy Filter Modifications Report

You can view Policy Filter Modifications directly from the Application Control reports. Privilege Manager automatically displays the previously viewed Policy Filter Modification report.

Note: To view a new report, click **Back to Policy Modification** at the top of the page to return to the Policy Modification page. Then select the associated policy and drill down to the filter details for review.

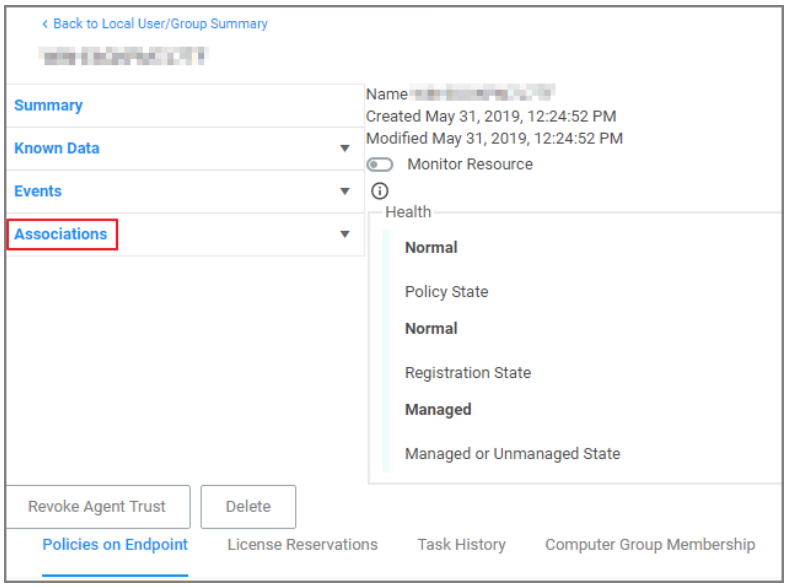


Primary User

The primary user is calculated by the data reported from the Logon Session inventory policy. The primary user is considered to be the user with the most minutes on the machine.

How to Find the Primary User for a Specific Machine

1. Navigate to your **Local User/Group Summary**.
2. Select the system for which you want to know the primary user.
3. Click **Associations**.

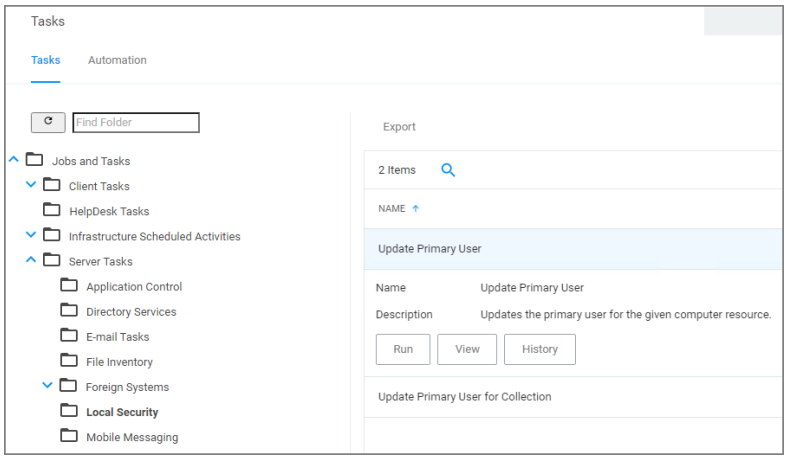


4. This will display the **Computer Primary User**.

Default Update Primary User for Collection

The default update primary user for collection task calculates the primary user on a schedule from inventory data.

1. Navigate to **Admin | Tasks**.
2. Expand **Server Tasks**.
3. Click **Local Security**.
4. From here you can run the **Update Primary User** or the **Update Primary User for Collection** Task.



Note: The Update Primary User Task only updates the primary user for a given computer resource.

Product Licenses

The Product Licenses report shows the number of licenses in use, per Operating System type (**OS TYPE**) configured in your application. OS types include both Windows and macOS clients.

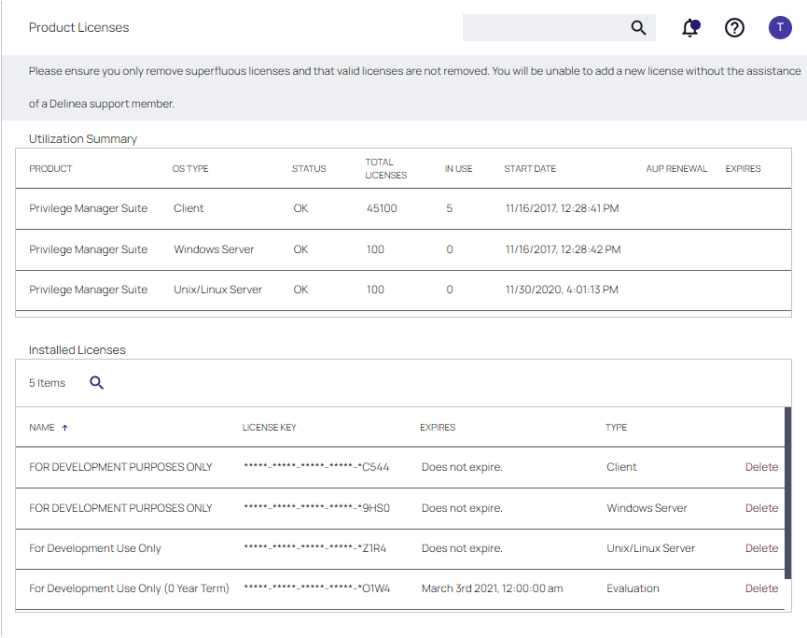
To access the report navigate to **Reports**, locate the **Diagnostic** reports group, and select **Licenses**.

A summary of all installed licenses is displayed, grouped by operating system.

Assessing Installed Licenses

To view details for any license count in an operating system, click the associated number in the **IN USE** column. A list of each license, its license key, type, and expiration is displayed. (Details are not displayed when **IN USE** is 0.)

Click **Delete** to delete any license.



The following factors may effect the number of licenses displayed:

- **Refresh** - License counts are periodically updated, and the count refreshed for the Utilization Summary. We recommend you recheck the count periodically for accuracy.

> **Note:** On the Home page, **AGENT POLICY STATE** displays counts for agents in a selected computer group, and does not directly relate to license usage. Therefore, this tile should not be used for a 1:1 comparison with the Utilization Summary of licenses in the Product Licenses report.

Reports and Queries

This topic provides an overview of the access and use of Privilege Manager **Reports and Queries**.

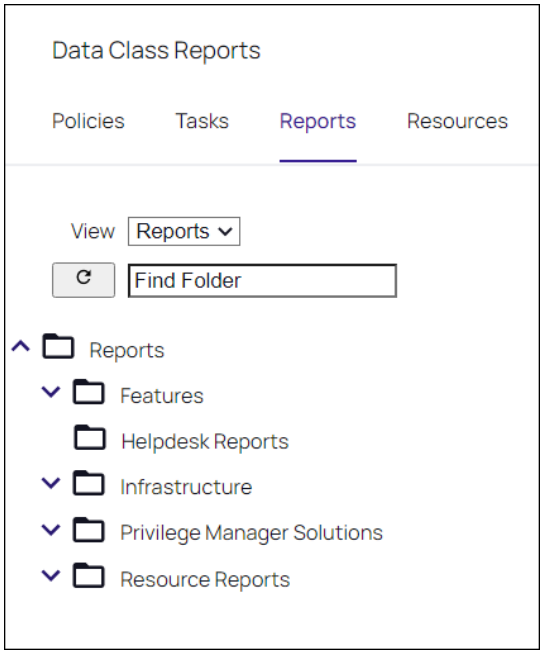
Privilege Managerexecutes SQL queries to produce reports. You can view existing (or canned) queries and generate resolved queries for testing purposes.

You also can run existing and custom reports external to the application using SQL Server Reporting Services, SQL Server Management Services, or a preferred tool.

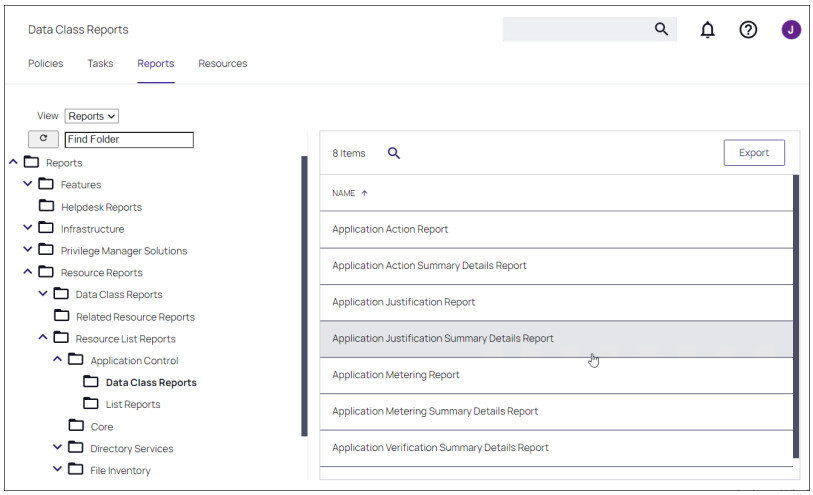
View Existing Privilege ManagerReports

Reports, accessible via the Privilege Manager left navigation pane, provides a categorized list of these items; in addition, **Select Report Options** allows you to hide or reveal reports by manipulating the switch associated with each.

You can view these reports by navigating to **Admin | Folders** and selecting the **Reports** tab, expanding to view the folder tree.



For example, **Application Justification Summary Details Report** is accessible via **Reports | Resource Reports | Resource List Reports | Application Control | Data Class Reports**.



Determine a Report's SQL Query Object

Each Privilege Manager report is a single XML object that references a separate XML object that contains the SQL query. By viewing the report object's XML, you can determine the SQL query object.

To view the report as an XML object, change the URL from:

`[Your_TMS_URL]/PrivilegeManager/#/item/view/9ba09fa5-ea7e-4352-8400-8eb58b8e41f9`

to:

`[Your_TMS_URL]/PrivilegeManager/#/item/xml/9ba09fa5-ea7e-4352-8400-8eb58b8e41f9`

st/TMS/PrivilegeManager/#/item/xml/9ba09fa5-ea7e-4352-8400-8eb58b8e41f9

‹ Back to Application Justification Summary Details Report

Application Justification Summary Details Report

Application Justification Summary Details Report


```
1  <Report xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/
2      <adc:Description>List all events representing actions for Application Control policies</adc:Description>
3      <adc:FolderId>0f59f691-ecc7-404c-8735-cb37a2423e69</adc:FolderId>
4      <adc:ItemId>9ba09fa5-ea7e-4352-8400-8eb58b8e41f9</adc:ItemId>
5      <adc:Name>Application Justification Summary Details Report</adc:Name>
6      <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
7      <adc:State i:type="adc:ItemState">
8          <adc:CreatedById>2dee6e6e-5098-44ac-ad36-6a1ae8fefea7</adc:CreatedById>
9          <adc:CreatedDate>
10             <dc:DateTime>2019-05-31T16:52:14.5247318Z</dc:DateTime>
11             <dc:OffsetMinutes>-420</dc:OffsetMinutes>
12         </adc:CreatedDate>
13         <adc:EffectiveSecuredId>a063e1d4-1876-4b6a-938e-00c476942ade</adc:EffectiveSecuredId>
14         <adc:EffectiveSecuredInheritedId>95ba3b94-bce2-40e9-b390-c8172d58d7dd</adc:EffectiveSecuredInheritedId>
15         <adc:IsCreated>true</adc:IsCreated>
16         <adc:ModifiedById>c44ad59e-9b47-4869-a1f5-295bfbcf8f96</adc:ModifiedById>
17         <adc:ModifiedDate>
18             <dc:DateTime>2020-06-02T14:38:11.2085195Z</dc:DateTime>
19             <dc:OffsetMinutes>-240</dc:OffsetMinutes>
20         </adc:ModifiedDate>
21         <adc:VisualStateId>ff2353f8-5880-5824-97be-71c44f116156</adc:VisualStateId>
22     </adc:State>
23     <adc:Strings />
24     <adc:Tags />
25     <ChartViews />
26     <ChildAssociations>
27         <arr:anyType i:type="adc:ItemAssociations">
28             <adc:AssociationTypeId>d819ac6c-1a7a-54b9-bbc0-752162e298f4</adc:AssociationTypeId>
29             <adc:AssociatedItemIds />
```


Edit

Upload Items File

Viewing an XML item helps determine the folder location, as detailed below. Viewing a report as XML also reveals the XML object for the SQL query.

Use your mouse to hover over the GUIDs in the XML, which displays the name of each GUID's object. Within the section for ChildAssociations, there is an Association for the report's Data Source. Hovering over the GUID for the AssociatedItemId reveals the report query name.

In the screenshot below, hovering over the GUID (9a3d82a3-c7be-47cc-aa1c-48acc7964620) identifies that Item as the **Application Justification Summary Details Report Query**.

```
26      <ChildAssociations>
27          <arr:anyType i:type="adc:ItemAssociations">
28              <adc:AssociationTypeId>d819ac6c-1a7a-54b9-bbc0-752162e298f4</adc:AssociationTypeId>
29              <adc:AssociatedItemIds />
30          </arr:anyType>
31          <arr:anyType i:type="adc:ItemAssociations">
32              <adc:AssociationTypeId>5b7800bc-7e4f-54ec-88b0-9797c09c5506</adc:AssociationTypeId>
33              <adc:AssociatedItemIds>
34                  <arr:guid>9a3d82a3-c7be-47cc-aa1c-48acc7964620</arr:guid>
35              </adc:AssociatedItemIds>
36          </arr:anyType>
37      </ChildAssociations>
38      <DefaultDataPresentation>Table</DefaultDataPresentation>
39      <LastRunDateTime>0001-01-01T00:00:00</LastRunDateTime>
```


Application Justification Summary Details Report Query

Clicking this GUID opens the XML for the query object in another tab on this screen:

Application Justification Summary Details Report | Application Justification Summary Details Report Query ×


```
1  <DataSourceItemContract xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schemas.microsoft.com/2003/
2      <adc:FolderId>b96eeb86-4846-45eb-9a36-504a3b70f774</adc:FolderId>
3      <adc:ItemId>9a3d82a3-c7be-47cc-aa1c-48acc7964620</adc:ItemId>
4      <adc:Name>Application Justification Summary Details Report Query</adc:Name>
5      <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
6      <adc:State i:type="adc:ItemState">
7          <adc:CreatedById>2dee6e6e-5098-44ac-ad36-6a1ae8fefea7</adc:CreatedById>
8          <adc:CreatedDate>
9              <dc:DateTime>2019-05-31T16:52:14.4153582Z</dc:DateTime>
10             <dc:OffsetMinutes>-420</dc:OffsetMinutes>
11         </adc:CreatedDate>
12         <adc:EffectiveSecuredId>8449e8ae-908b-4205-802b-dcc05b57d756</adc:EffectiveSecuredId>
13         <adc:EffectiveSecuredInheritedId>17969920-3bc4-4a44-89c4-44b62aab01f8</adc:EffectiveSecuredInheritedId>
14         <adc:IsCreated>true</adc:IsCreated>
15         <adc:ModifiedById>c44ad59e-9b47-4869-a1f5-295bfbcf8f96</adc:ModifiedById>
16         <adc:ModifiedDate>
17             <dc:DateTime>2020-06-02T14:38:11.1205194Z</dc:DateTime>
18             <dc:OffsetMinutes>-240</dc:OffsetMinutes>
19         </adc:ModifiedDate>
20         <adc:VisualStateId>1199377a-1cbf-556d-a669-5effa21fa04c</adc:VisualStateId>
21     </adc:State>
22     <adc:Strings />
23     <adc:Tags />
24     <DataSource i:type="RawSqlDataSource">
25         <Name>Application Justification Summary Details Report Query</Name>
26         <Parameters>
27             <adcp:Parameter>
28                 <adcp:DataType>System.String</adcp:DataType>
29                 <adcp:DefaultValue mss:type="mss:string">EN</adcp:DefaultValue>
```


Edit | Delete

Upload Items File

The XML object for the query includes the direct SQL query that the application runs. However, viewing the query in Privilege Managerprovides more reliable query results.

View a SQL Query in Privilege Manager

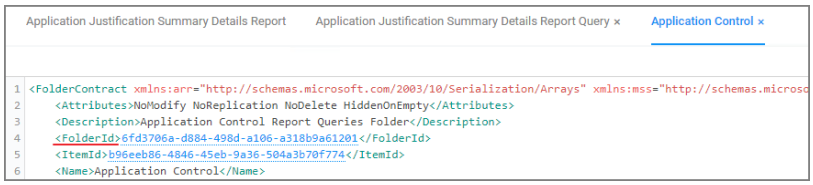
You can view the Privilege Manager SQL queries via **Admin | Folders**; however, it is helpful to know the folder location for specific queries. In the XML object for the query, hover over the GUID associated with the **FolderId** and select.

Application Justification Summary Details Report | Application Justification Summary Details Report Query ×

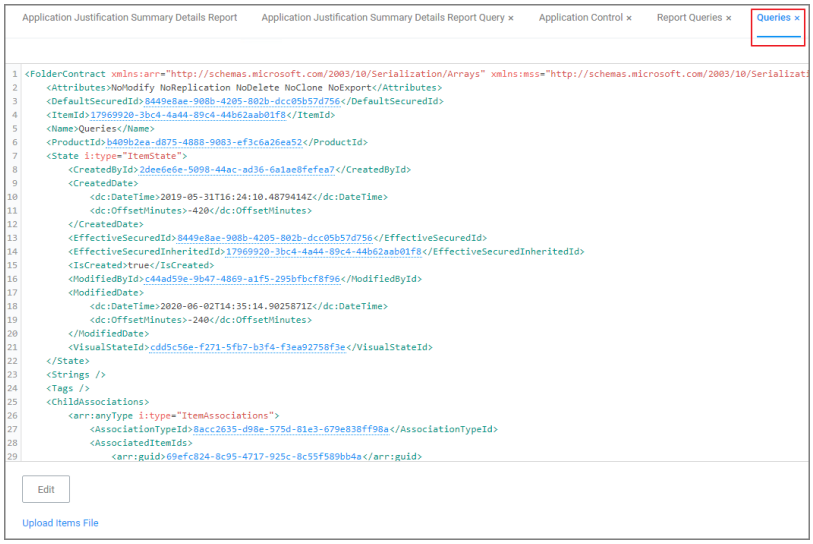

```
1  <DataSourceItemContract xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schemas.m
2      <adc:FolderId>b96eeb86-4846-45eb-9a36-504a3b70f774</adc:FolderId>
3      <adc:ItemId>9a3d82a3-c7be-47cc-aa1c-48acc7964620</adc:ItemId>
4      <adc:Name>Application Justification Summary Details Report Query</adc:Name>
5      <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
6      <adc:State i:type="adc:ItemState">
```


Application Control

This action opens the XML folder that contains the query.



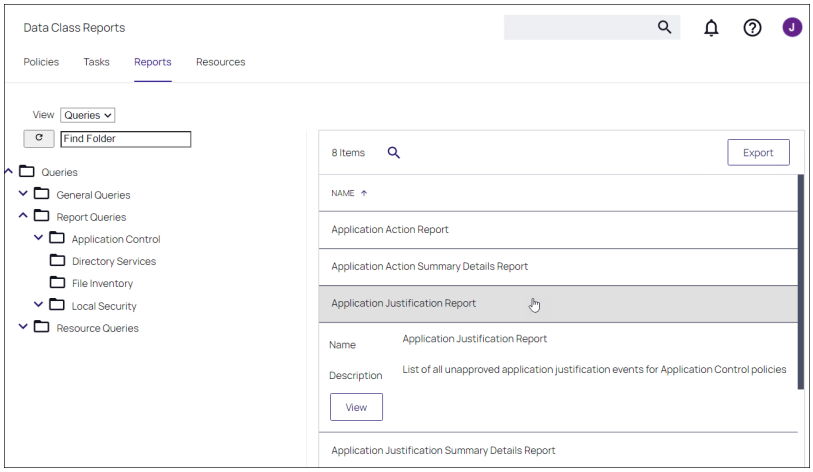
Click **FolderId** to open the XML for its parent folder and continue until reaching the root folder, which will not have a **FolderId** attribute. For the SQL queries, the root folder is **Queries**.



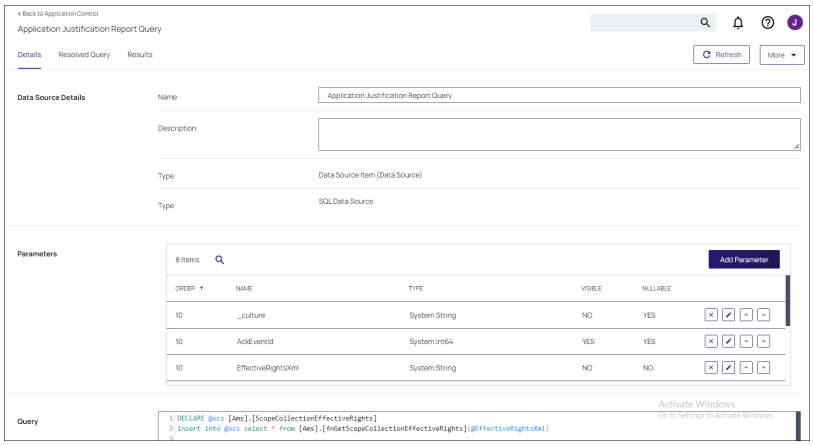
This XML view now displays the full folder location of this query: **Queries | Report Queries | Application Control**.

Access and Edit a Query from the Folder View

Navigate to **Admin | Folders** and select the **Reports** tab. From the **View** drop-down list box, select **Queries**. Navigate the folder structure determined above: **Queries | Report Queries | Application Control**. Select the **Application Justification Report Query** from the center pane.



View this query object. The **Query** tab displays the SQL query that the application runs. This is the same query that appears in the XML of the object.



Scroll to the lower section of the page to edit the query XML.

Resolved Query

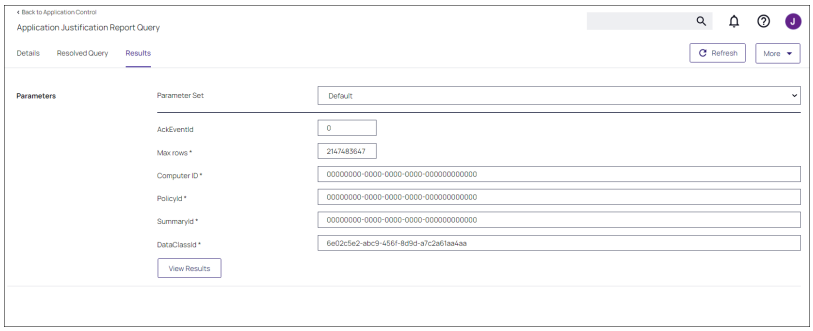
The **Resolved Query** tab provides queries you can use directly on the database to return similar results that the application receives when it runs the query in the object - facilitating your ability to run or customize queries in SQL Server Reporting Services.

On the **Resolved Query** tab, sliding the **Show as Anonymous Block** switch to the right or **Yes** position assigns values to the parameters the query uses. From the **Parameter Set** drop-down list box, select **Test** to assign the parameters with appropriate values to run this query directly on your database.

Click **Copy To Clipboard** and then paste the resolved query in SQL Server Reporting Services, SQL Server Management Services, or your preferred tool.

Results

The **Results** tab provides options to change query information.



You can change the **Parameters** and enter specific item Ids.

Troubleshooting

This section contains a collection of troubleshooting articles to help with problems that might occur in your Privilege Manager integration/instance.

The following troubleshooting topics are available:

Installation and Upgrade Issues

- Troubleshooting Installation Issues
- 10.5 Folder Permission for MachineKeys
- Retrieving the COM class factory error
- Database Connection Issue during Setup
- Supporting Multiple TLS Versions

Agents Troubleshooting

- Agent Registration Error Following an OS Upgrade
- "Agent 404 Error: Service Startup Change" on page 224
- Running updateclientitems.ps1 on an Agent Triggers an Error
- Client Item List Downloads
- Advanced Messages not Working for Child Processes of Microsoft Edge

Workstation Troubleshooting

- Endpoint Troubleshooting
- How to Recover an Unresponsive macOS Endpoint

- Catalina FileSystemWatcher Issue

Privilege Manager Logs

- Where are My Server Logs?
- Where are My Agent Logs?
- SQL Server Transaction Log
- User Interface and Ports

Performance Issues

- Improve Boot-up Performance
- Unable to access Privilege Manager

Errors

- Common Errors
- Error: Could not allocate space for object
- UI Storage Error Message
- Notify User Justification failed
- Invalid Product Identifier
- Installation Hangs with Error: Worker Role Monitor received exception during ping

Troubleshooting Tools

- How to use the Thycotic Monitor for Troubleshooting
- Using Process Hacker for Troubleshooting
- Troubleshooting a Policy with Process Explorer

Errors

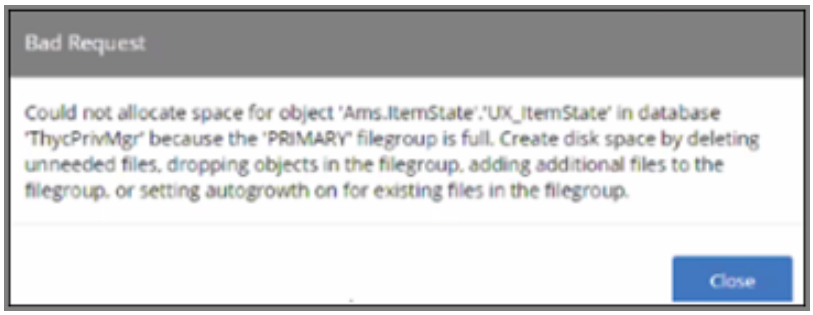
The following topics about error messages in Privilege Manager are available:

- Common Errors
- Error: Could not allocate space for object
- UI Storage Error Message
- Notify User Justification failed
- Invalid Product Identifier
- Installation Hangs with Error: Worker Role Monitor received exception during ping

Error: Space Allocation

This topic describes the following error while working with Privilege Manager:

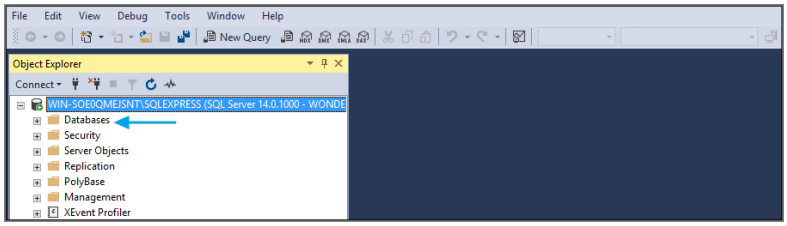
Could not allocate space for object 'Ams.ItemState'.'UX_ItemState' in database 'ThycPrivMgr' because the 'PRIMARY' filegroup is full.



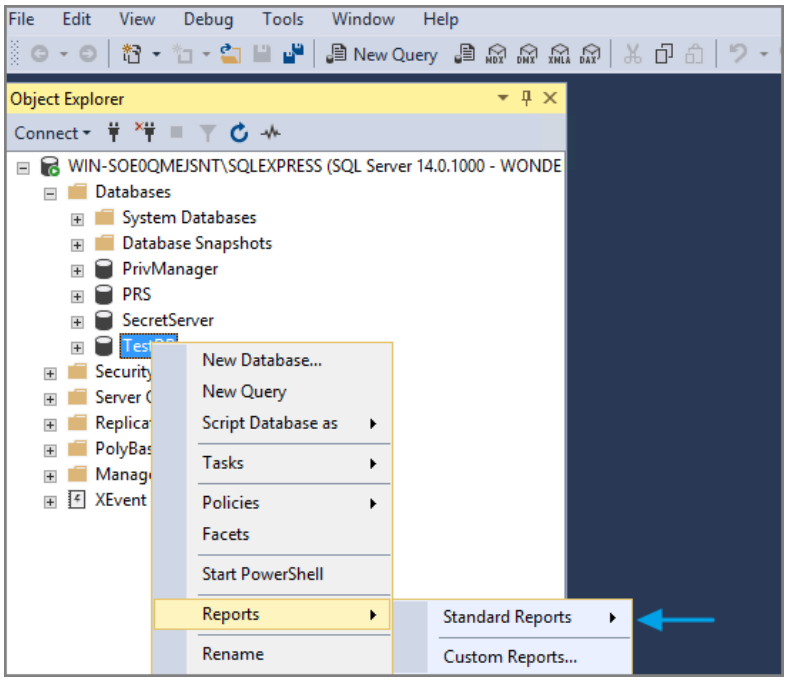
The error indicates that either the Privilege Manager database is full and out of space or the database server running is out of space.

Resolving the Error

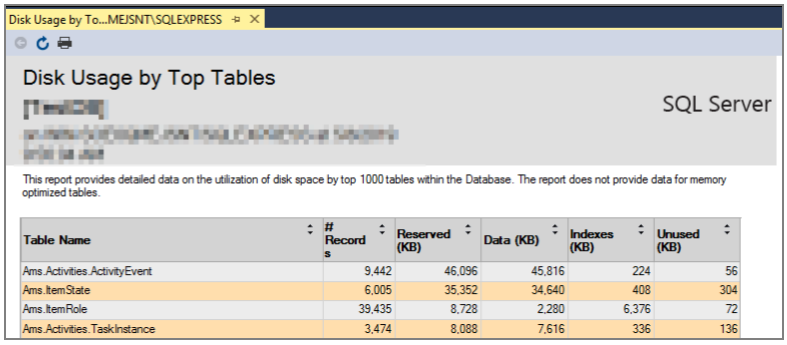
1. Navigate to SQL Server Management Studio.
2. Click **Connect**.
3. Expand Databases.



4. Right-click the Privilege Manager database, select **Reports**.
5. Select **Standard Reports**.



6. Select **Disk Usage by Top Tables** report.



7. The report shows the top tables by data usage.
8. If the top table does contain a lot of data, locate the table that contains the highest number of files and open a support case. Provide the information collected with a screen shot of the report to determine the best way to reduce the size of the table.

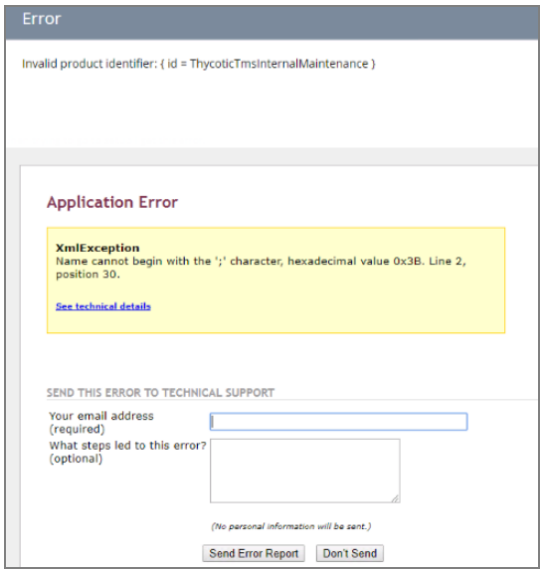
   If the top tables do not contain a lot of data, the issue could possibly be:

   - The database server is running out of disk space. You can check to see what drive the database is stored on to see how much space is left. This will be specific to your environment regarding disk space.
   - Check if there are other databases on the same server and investigate if a different database is taking up space.

Error: Invalid product identifier: { id = thycoticTmsInternalMaintenance }

When attempting to upgrade Privilege Manager, you receive the following error:

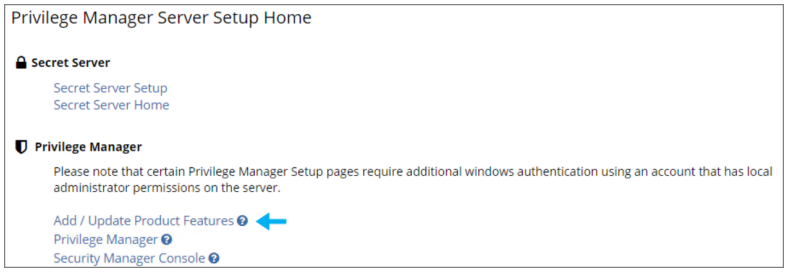
Error: *Invalid product identifier: { id = thycoticTmsInternalMaintenance }*



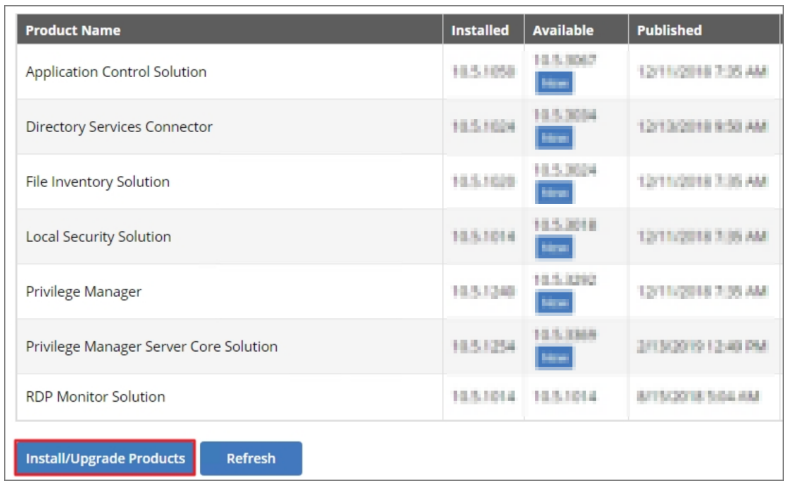
Resolve

1. Navigate to `https://[YourInstanceName]/TMS/Setup`.
2. Click the **Upgrade Banner** at the top of the Privilege Manager Home page.

3. Click **Add / Update Product Features**.



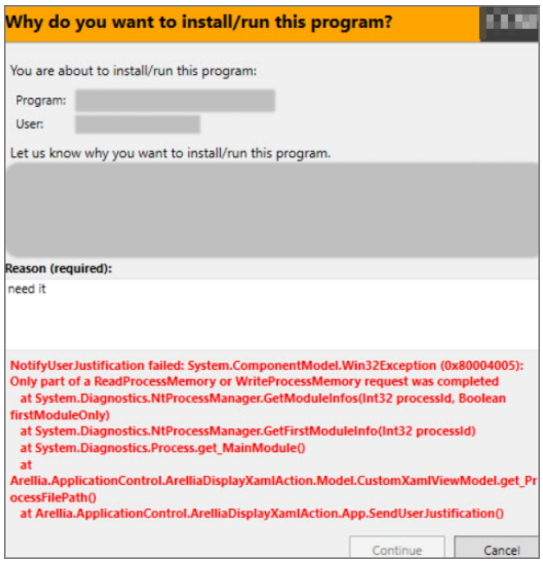
4. Click **Install/Upgrade Products**.



5. Select **ALL** of the required solutions.
6. Click **Install** and the upgrade process will begin.

Notify User Justification failed

You receive the following error when users attempt to run a program with a policy that uses the action for Notify User justification.



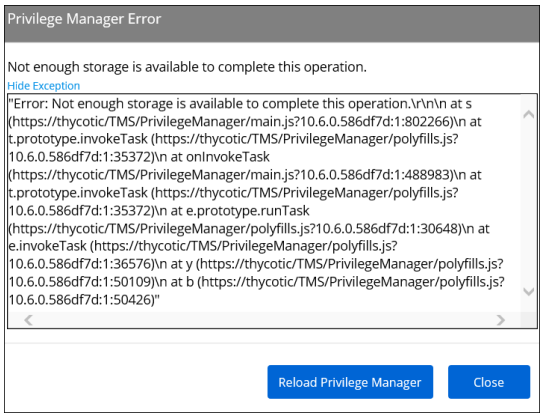
Resolve

1. Either disable the Anti-Virus Real time scan.
2. Or, set Anti-Virus Real-time scanning exclusions.

UI Storage Error

You might have to clear your browser cache if you get the following error in the Privilege Manager console:

Not Enough Storage is available to complete this operation



Resolution

1. Open your browser window and clear the cache.
2. Close and re-open the browser
3. Launch Privilege Manager and re-try the action.

   Note: If the error continues, open a different browser and try to replicate the error. Save any screenshots and open a support case.

4. If this occurs while on the server, please ensure that there is enough disk space to complete the action.

Common Errors

Access Denied

Error: *Access Denied. You do not have permission to view this directory or page using the credentials that you supplied*.

To Resolve:

After logging in to Privilege Manager 10.3 with a user account that has Privilege Manager Administrator Role rights, if you experience this error, verify if SSL 3.0 and/or TLS 1.0 have been disabled. If those protocols have been disabled on the server, you'll need to replace `C:\inetpub\wwwroot\Tms\bin\Thycotic.Owin.Security.dll` with `http://tmsnuget.thycotic.com/scripts/Thycotic.Owin.Security.dll`

Recycle the TMS Application Pools in IIS and attempt to access Privilege Manager again.

Server Error in...

Error: *Server Error in '/' Application. Runtime Error*

Your Secret Server instance doesn't have the correct URL pointing at Privilege Manager.

To Resolve:

Go to yourSecret Server instance (Tools |Secret Server), then **Admin** | **Configuration**. Verify that your TMS Installation URL is set to ~/../TMS.

SSL Connectivity or Certificate Issues

Error: *SSL Connectivity or Certificate Issues?*

Trusting an SSL Certificate on a Client Machine (KB)

When a self-signed certificate is installed on a server for the Secret Server website, client computer browsers will generally give security warnings for that web site. This is because for public websites, only certificates issued by trusted authorities can be trusted as valid certificates. For certificates that will only be used within a company or domain, self-signed certificates the security warnings can generally be ignored.

However, the security warnings can also interfere with the use of the Secret Server Launcher and Web Password Filler.

To Resolve:

The certificate can be installed on the client machine either through Internet Explorer or Certificates snap-in.

The following steps can be used to trust the certificate:

1. Make sure that the host to which the certificate is issued is the same as the host name for your Secret Server website.
   - Open Internet Explorer and navigate to Secret Server.
   - Click **Continue** to this website if you are prompted.
   - Click the Certificate Error icon next to the navigation bar and then click **View certificate**. The value next to Issued to should match the host name for your website. For example, if your website is `https://www.mydomain.local/SecretServer`, it should say "Issued to: www.mydomain.local". If these fields do not match, the client will not be able to fully trust the certificate.
2. Obtain a copy of the certificate file and transfer it to the client computer.
   - On the server that Secret Server is installed on, find **Run** from the start menu or screen and type in mmc, then press **Enter**.
   - From the **File** menu, select **Add/Remove Snap-in**.
   - Select the Certificates snap-in, then click the right arrow button to add it.
   - In the window that appears, select **Computer Account**, then **Local Computer**, and then click **Finish**.
   - You should now see the **Certificates (Local Computer)** node. Expand the **Personal** folder and then the **Certificates** folder under it.
   - Right-click the certificate that Secret Server uses, then click **All tasks** and select **Export**.
   - Keep clicking **Next** to accept defaults in the wizard. Enter a filename, and then click **Finish**. The certificate has now been exported.
   - Copy the certificate from your server and transfer it to your client computer.

     Note: If you have Firefox, the certificate can be saved to your client computer by viewing and exporting it after navigating to the website.
3. Install the certificate on the client computer.

- On the client computer, find **Run** from the start menu or screen and type `mmc`, then press **Enter**.
- From the File menu, select **Add/Remove Snap-in**.
- Select the **Certificates** snap-in, then click the right arrow button to add it.
- In the window that appears, select **My user account**, and then click **Finish**.
- Expand the **Trusted Root Certification Authorities** folder, then right-click the **Certificates** folder, and select **All Tasks** | **Import**.
- Click **Next** and **Yes** to accept default settings for all steps of the wizard.
- When prompted for the certificate file, select the file you saved in the previous step (2).

Note: You may need to reopen Internet Explorer and browse to Secret Server once more to see the change reflected on the client machine.

Granting Permissions on New SSL Certificate for Privilege Manager (KB)

If you change your certificate or if it is automatically renewed, you may need to grant permissions on your new SSL certificate to the service account that the TMS app pools run under. TMS accesses the SSL certificate to sign all of the policies that Privilege Manager sends out to agents, adding an extra security layer to your environment.

Messages you may see include:

- https: does not render
- Navigating to Https://[ServerName]/TMS/PrivilegeManager loads a blank screen
- Agents stop receiving configuration information from the Privilege Manager Web Server
- Http : TMS requires an https (SSL) / secure connection

For the fastest resolution to Permissions issues, you can run a PowerShell script:

- Navigate to your TMS Website on your Privilege Manager web server (Usually located in `c:\inetpub\wwwroot\`), then navigate to `Tms\App_Data\Tools\SSLHelper.ps1` on your Privilege Manager web server, right-click this and select **Run** with PowerShell to execute.

To grant permissions manually, follow these steps

1. Using MMC on your Privilege Manager web server, open the certificates snap-in (**File** | **Add/Remove Snap-in...** | **Certificates** . Click **Add**), then select the computer account to manage the local computer. Click **Next**, then **Finish** and **OK**.
2. Double-click **Certificates (Local Computer)** and locate the certificate that your TMS site is using (it will most likely be under **Personal** | **Certificates** , unless you specified a different location*)
3. Right-click the certificate and select **All Tasks** | **Manage Private Keys**.

Grant Read Access to the account(s) that TMS is running under

If this is a user account then you may adjust permissions to the user account. To check, go to your app pool in IIS, right-click the IIS app pool **Advanced Settings...** Identity row: if your app pool identity is listed as something OTHER THAN **ApplicationPoolIdentity** in IIS (i.e., Delinea |ServiceAccount), then your app pool is using a user account.

If this IS the Application Pool Identity (i.e., not a user account) you will need to adjust permissions to three app pools: IIS AppPool\TMS, IIS AppPool\TMSWorker and IIS AppPool\TMSAgent. Note that names of app pools may vary depending on your environment.

Recycle your TMS, TMSAgent, and TMSWorker app pools in IIS.

Note: If you are unsure which certificate matches the one you are using in IIS, follow these steps to ensure your certificate thumbprints match:

In IIS, on your Privilege Manager web server, navigate to the site you are using to run Privilege Manager. Right-click on this site, click **Bindings**. Choose the https port you need to update and select **Edit**. View the SSL Certificate this is attached to.

Next, choose the **Details** tab and scroll down to find the certificate's thumbprint. Copy the list of numbers and letters that make up your certificate's thumbprint (a SHA256 hash).

Return to your certificates in MMC (step 2 above). Right-click **Certificates (Local Computer)** and select **Find Certificates...**.

In the **Contains** box, paste your thumbprint SHA256 hash and select SHA256 from the Look in Field drop-down. Click **Find Now**. This returns the certificate name that your Privilege Manager Binding is currently linked to.

Tasks Stuck at Ready

Error: *Are your tasks sitting at "Ready" for extended periods of time?*

To Resolve:

1. Navigate to **Admin** | Configuration | **Advanced** and make sure the URL for the Monitor Worker Role are accurate for the bindings (Check the hostname in the Base local address and the Port).
2. Open IIS Manager, check to make sure the app pools have Read access to the certificate that you've assigned to that binding via MMC Certificates plug-in. More instructions on how to do this in our Granting Permissions on New SSL Certificate for Privilege Manager KB, posted here.
3. Manually recycle the TMS and TMS Worker app pools.

CPU Issue

Error*: CPU overworked in your Agent or 'Unexpected failure in ACS Agent background'*

Your agent may be configured incorrectly.

To Resolve:

1. In Privilege Manager navigate to **Admin** | **Agents**.
2. Under the **Windows** tab, verify that your **Send Application events every** and **Refresh Client item cache every** settings are both set to 0.
3. Save changes, refresh your client item cache, enforce the update on your endpoint machine (Follow the update PowerShell script instructions listed under *How do I Update Specific Agents Immediately*? above).

System Critical Error

Error: *System Critical Error - execute/PolicyDetailComponent* in Firefox

To Resolve:

Open Privilege Manager in a different browser, such as Chrome or Internet Explorer 11. If you prefer Firefox as your web browser, download this zip file: `http://tmsnuget.thycotic.com/scripts/firefox.fix.zip` Unzip these files, then copy and paste into `C:\inetpub\wwwroot\Tms\Spa\PrivilegeManager\` on your Privilege Manager Server.

Refresh your Firefox browser.

Installation Hangs with Error: Worker Role Monitor received exception during ping

During the installation of Privilege Manager the install hangs and is unable to proceed to the next step of the installation.

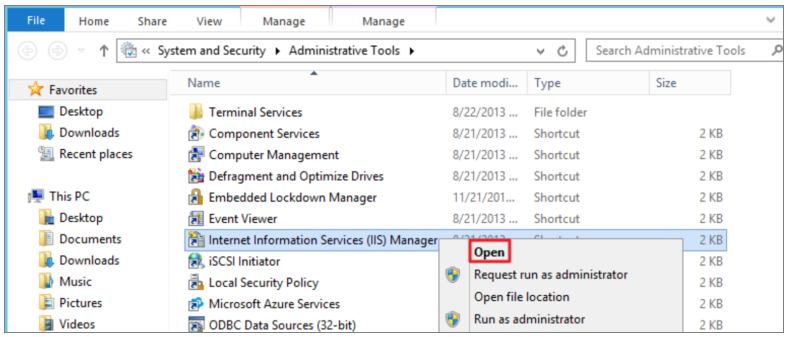
After checking the Thycotic Monitor, you see the below error in the log viewer:

Worker Role Monitor received exception during ping: The HTTP request is unauthorized with client authentication scheme 'Negotiate'. The authentication header received from the server was 'Negotiate,NTLM'

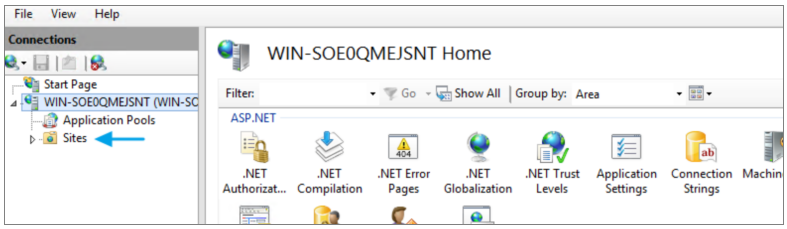
Note: This error is due to a host name in the binding within IIS.

Resolve

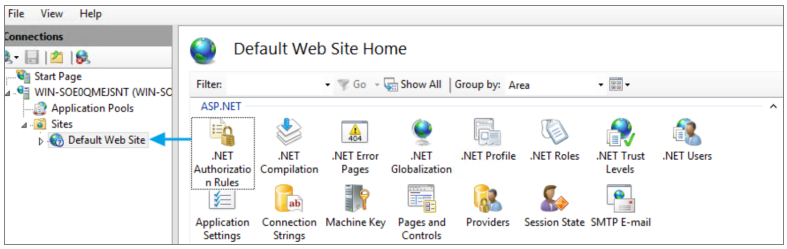
1. Open **Internet Information Services (IIS) Manager**.



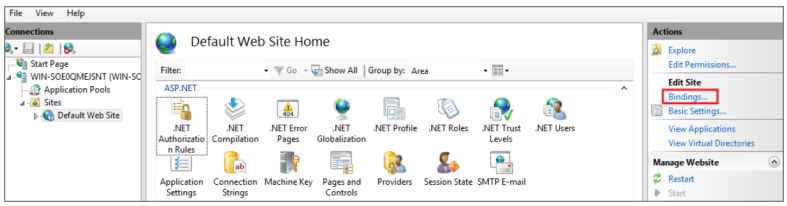
2. Expand down to **Sites**.



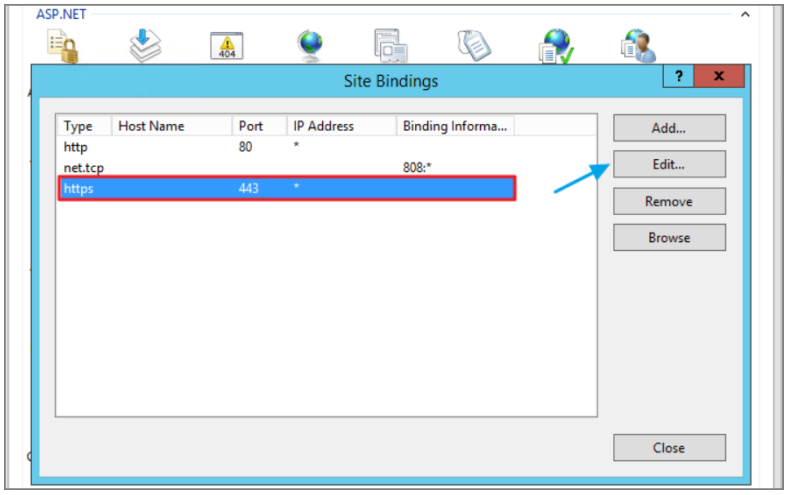
3. Click **Default Web Site** or the **top node site**.



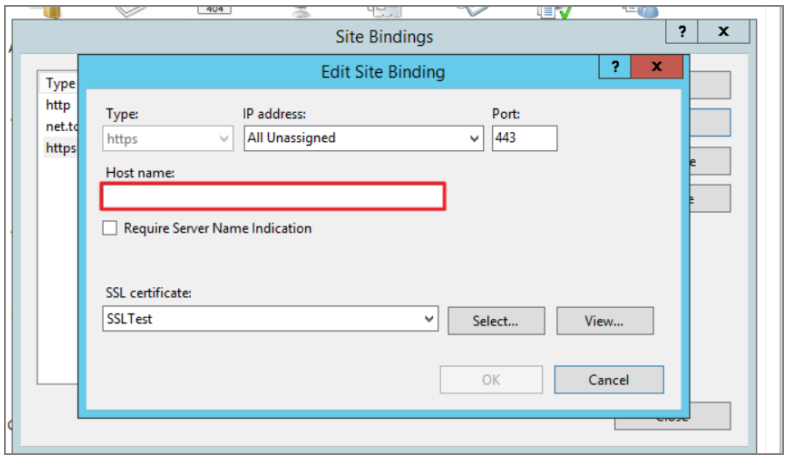
4. Click **Bindings**.



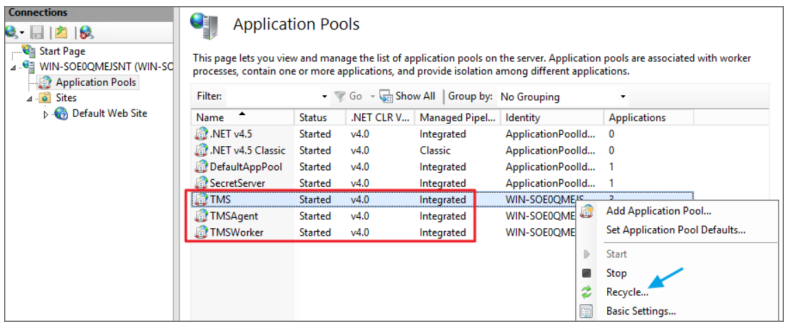
5. Select the **HTTPS binding**. Click **Edit.**



6. Confirm that there is no **Host name** included for the HTTPS binding for the TMS site. If so, please delete it.



7. **Recycle** all the TMS application pools in IIS.



8. Try the install again by going to **https://localhost/TMS/Setup**.

Installation and Upgrade Issues

The following topics are available:

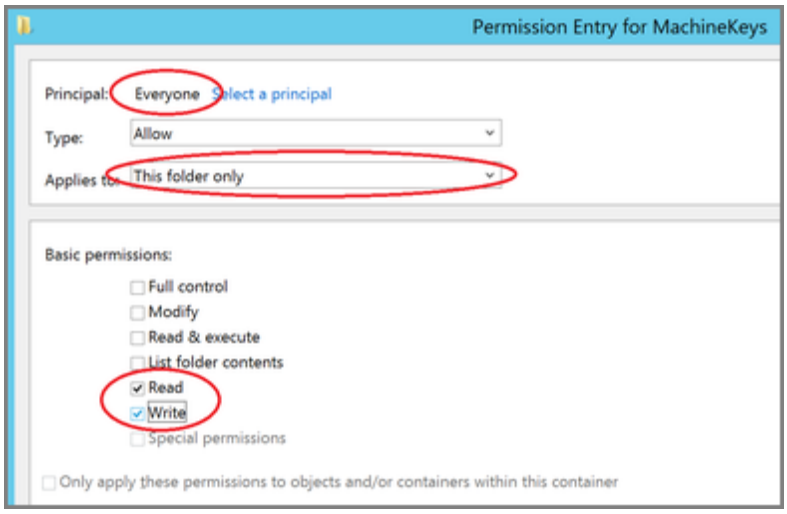
- Troubleshooting Installation Issues
- 10.5 Folder Permission for MachineKeys
- Retrieving the COM class factory error
- Database Connection Issue during Setup
- Supporting Multiple TLS Versions

10.5 Folder Permissions - MachineKeys

During installation of Privilege Manager 10.5 (or an upgrade from prior versions) Privilege Manager attempts to create a new self-signed certificate for internal use. If permissions on the folder `%ProgramData%\Microsoft\Crypto\RSA\MachineKeys` are incorrect, the install fails with a cryptographic exception and the text **Access Denied**.

Follow the steps below to add Everyone (Read, Write, This Folder Only) permissions to `%ProgramData%\Microsoft\Crypto\RSA\MachineKeys`.

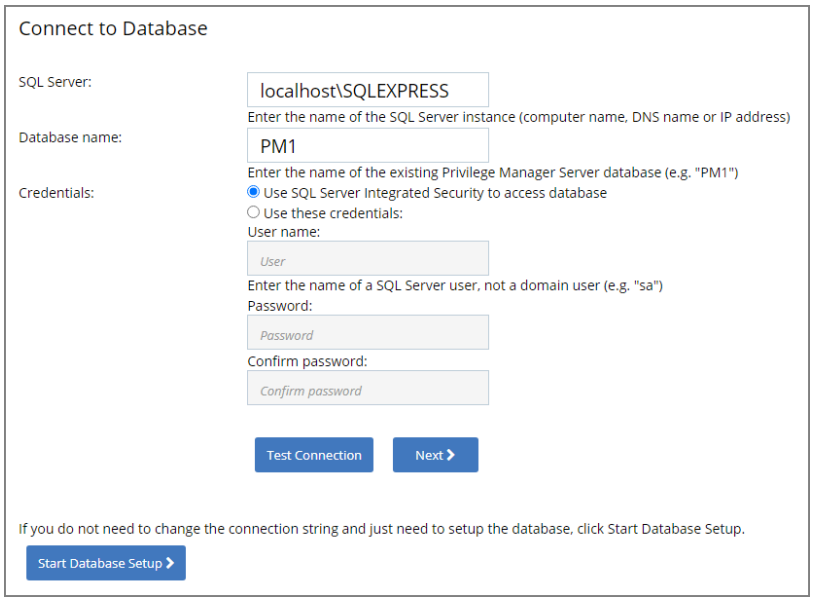
1. Browse to `%ProgramData%\Microsoft\Crypto\RSA\MachineKeys`.
2. Right-click on the folder and select **Properties**.
3. Select the **Security** tab and click the **Advanced** button.
4. On the **Permissions** tTab, click the **Change permissions** button. (If you are already running as an administrator, you may not need this step.)
5. On the **Permissions** Tab, click **Add**.
6. On the next dialog, click the **Select a principal** link.
7. In the **Enter the object name to select** field, type **Everyone** and click **OK**.
8. You will see the dialog shown below, select **This folder only** and **Read and Write**.



9. Click **OK** to add the entry.
10. Click **Apply** to apply the changes.
11. Navigate back to the Privilege Manager Setup page and select the repair option for the Privilege Manager Server Core Solution.

Databased Connection Issued during Setup/Update

When accessing the Privilege Manager console or during an instance update, if one of the databases is unreachable the user is directed to the Connect to Database page.



Reasons for this state:

- The SQL Server service is not reachable. Check the service and restart if necessary.
- The SQL Certificate has expired. Delete the old certificate and have the server recreate the certificate.
- SQL Server authentication method changed. Depending on the selection during initial setup, the credentials used come from either:
  - SQL Integrated Security settings and no further details need to be entered when the first radio button is selected. This is usually the account information for the account running the application pools for Privilege Manager in IIS.
  - Overwrite Account credentials when the second radio button is selected.

If a database connection ever needs to be updated, the Connect to Database page can be accessed locally on the server hosting the Privilege Manager instance by navigating to `.../TMS/Setup/Database/ConnectDatabase` in the browser. To access the page, the user needs to have local admin rights on the server.

Supporting Multiple TLS Versions

Privilege Manager on-premise does not work with Azure Service Bus if the web server is set to use only TLS 1.2.

Customers that want to restrict connections on their web server to TLS 1.2 need to make modifications to `C:\inetpub\wwwroot\Tms\ServiceBus\web.config` and `C:\inetpub\wwwroot\Tms\Worker\web.config`. They also must have .NET Framework 4.6 or newer installed and modify the <system.web> section as follows:

1. Open `C:\inetpub\wwwroot\Tms\ServiceBus\web.config`.
2. Change the <system.web> section to:

```
<system.web>
```

```
 <httpRuntime targetFramework="4.6"/>  <authorization>   <allow
users="?"/>  </authorization> <authentication mode="Windows"/></system.web>
```

3. Save the file.
4. Open `C:\inetpub\wwwroot\Tms\Worker\web.config`.
5. Change the <system.web> section to:

```
<system.web>
 <httpRuntime targetFramework="4.6"/>  <authorization>   <allow
users="?"/>  </authorization> <authentication mode="Windows"/></system.web>
```

6. Save the file.

Retrieving the COM Class Factory Error

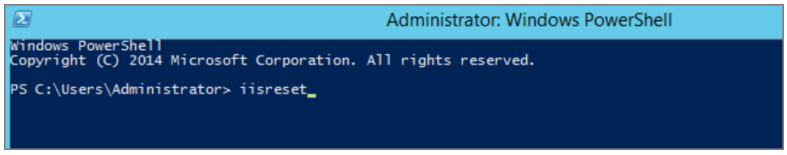
While attempting to upgrade Privilege Manager, you receive an error message when accessing `https://[YourInstanceName]/TMS/Setup`.

The window is unable to load with the following error message:

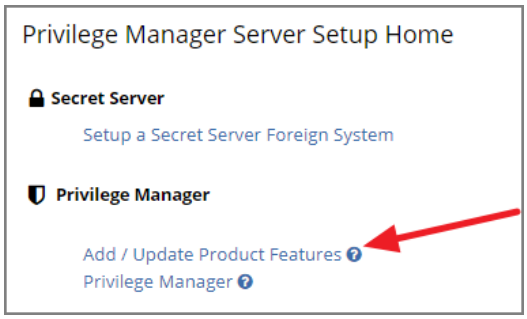
```
“Server Error in '/Tms/Setup' Application.

Retrieving the COM class factory for component with CLSID {228FB8F7-FB53-4FD5-8C7B-
FF59DE606C5B} failed due to the following error:
800703fa Illegal operation attempted on a registry key that has been marked for deletion.
(Exception from HRESULT: 0x800703FA).”
```

Resolve

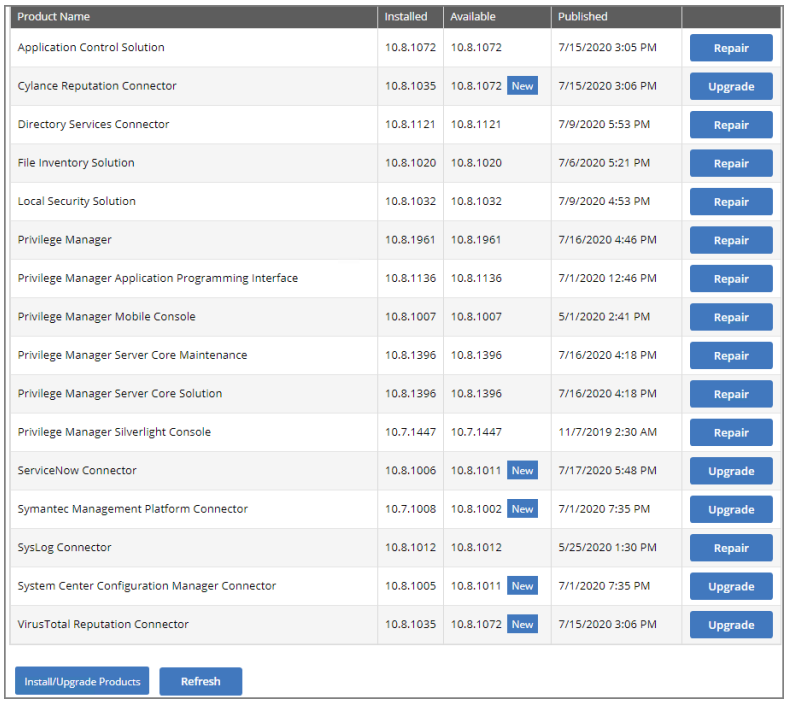
1. Close the browser window.
2. Complete an IIS reset by searching for the Windows PowerShell application.
3. Right-click and select **Run as Administrator**.
4. Enter: **IISreset** |. Press **Enter**.



5. Once the IIS reset has completed navigate back to `https://[YourInstanceName]/TMS/Setup`.
6. Click **Add / Update Product Features**.



7. Click **Install/Upgrade Products**.



Product Name	Installed	Available	Published	
Application Control Solution	10.8.1072	10.8.1072	7/15/2020 3:05 PM	Repair
Cylance Reputation Connector	10.8.1035	10.8.1072 New	7/15/2020 3:06 PM	Upgrade
Directory Services Connector	10.8.1121	10.8.1121	7/9/2020 5:53 PM	Repair
File Inventory Solution	10.8.1020	10.8.1020	7/6/2020 5:21 PM	Repair
Local Security Solution	10.8.1032	10.8.1032	7/9/2020 4:53 PM	Repair
Privilege Manager	10.8.1961	10.8.1961	7/16/2020 4:46 PM	Repair
Privilege Manager Application Programming Interface	10.8.1136	10.8.1136	7/1/2020 12:46 PM	Repair
Privilege Manager Mobile Console	10.8.1007	10.8.1007	5/1/2020 2:41 PM	Repair
Privilege Manager Server Core Maintenance	10.8.1396	10.8.1396	7/16/2020 4:18 PM	Repair
Privilege Manager Server Core Solution	10.8.1396	10.8.1396	7/16/2020 4:18 PM	Repair
Privilege Manager Silverlight Console	10.7.1447	10.7.1447	11/7/2019 2:30 AM	Repair
ServiceNow Connector	10.8.1006	10.8.1011 New	7/17/2020 5:48 PM	Upgrade
Symantec Management Platform Connector	10.7.1008	10.8.1002 New	7/1/2020 7:35 PM	Upgrade
SysLog Connector	10.8.1012	10.8.1012	5/25/2020 1:30 PM	Repair
System Center Configuration Manager Connector	10.8.1005	10.8.1011 New	7/1/2020 7:35 PM	Upgrade
VirusTotal Reputation Connector	10.8.1035	10.8.1072 New	7/15/2020 3:06 PM	Upgrade

Install/Upgrade Products Refresh

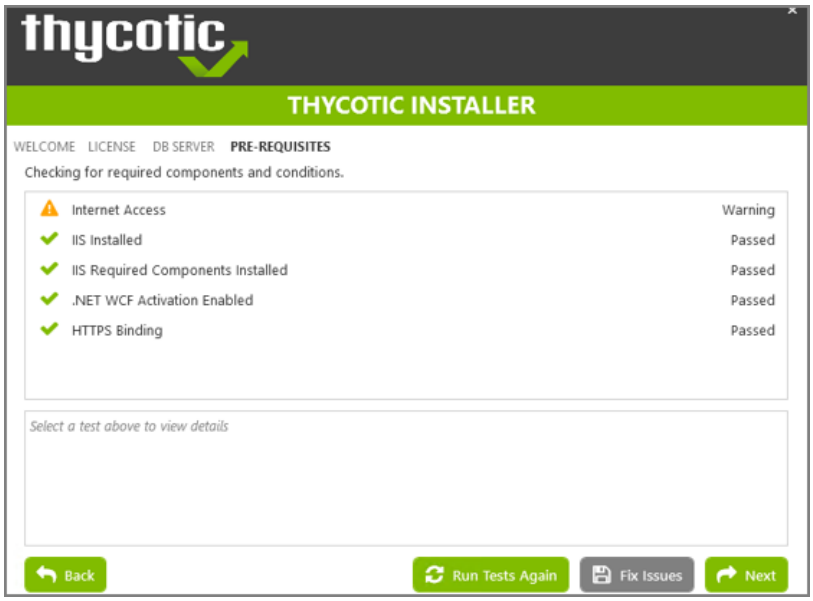
8. Select **ALL** required solutions.
9. Click **Install** and the upgrade process will begin.

Installation Issues

This article provided troubleshooting tips to help anyone who hits a snag during an install for Privilege Manager.

Internet Connection

If your server is not connected to the internet, you see the following:

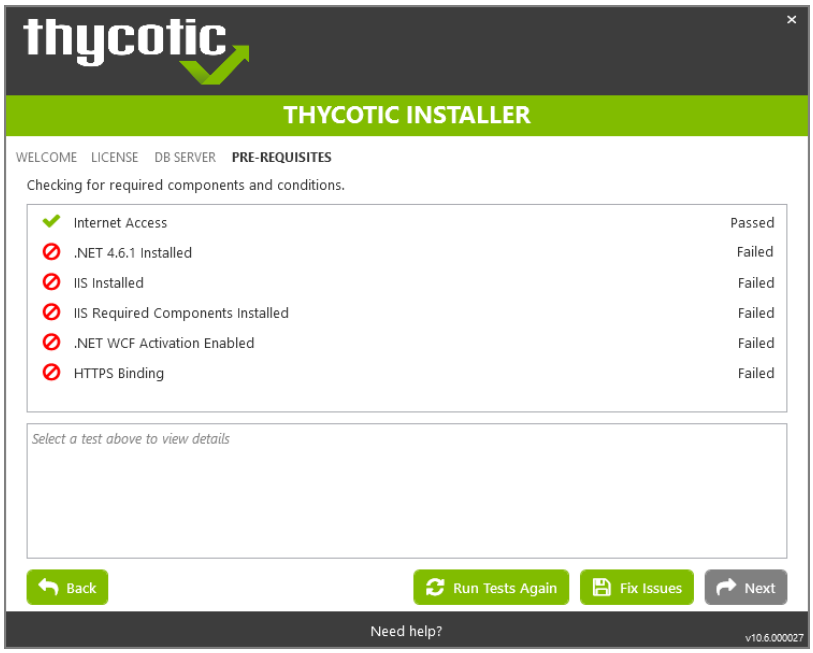


To Resolve:

Click **Next** to proceed through your installation offline.

.NET Dependency

Don't have the required .NET version Dependency installed to accompany your SQL DB? This is what you will see:

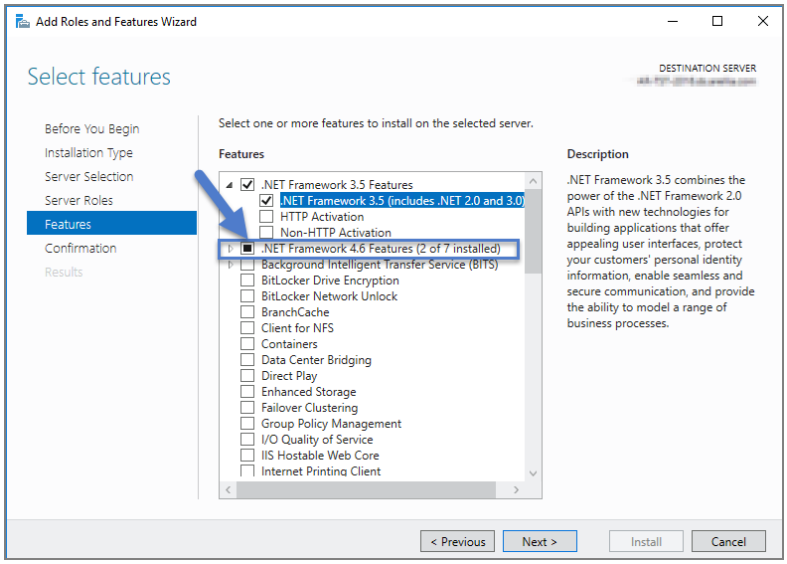


To Resolve:

Click the **Fix Issues** button on the Delinea Installer, then run the pre-requisites check again.

If the error persists, manually install the recommended .NET version.

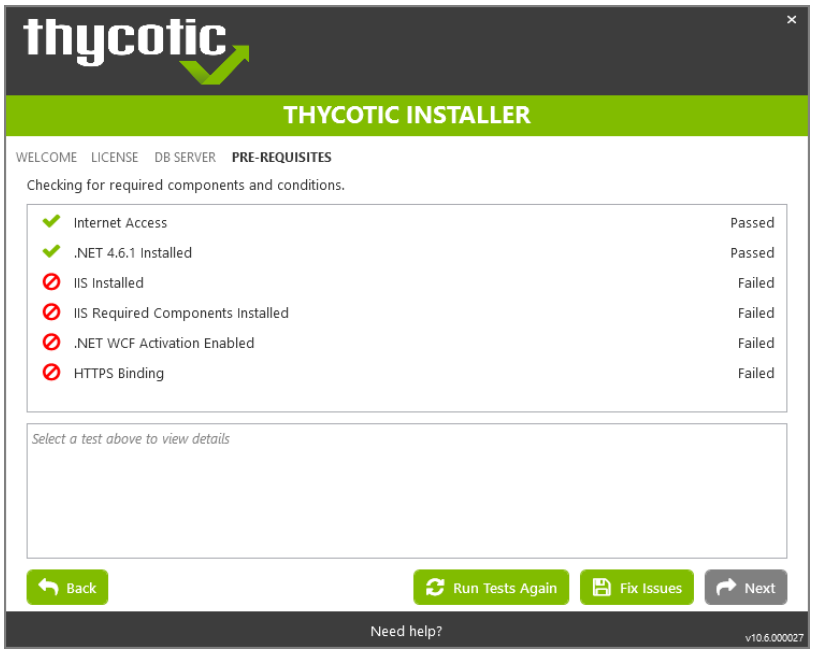
1. Open your Server Manager, in the upper right side of the screen, click **Manage**, then **Add Roles** and **Features** from the drop-down list. This opens your **Add Roles** and Features Wizard. Verify that the correct Destination Server is listed in the upper right-hand side of the screen.
2. Click **Next** through the wizard steps, until you arrive on the Features page.
3. Check the box next to the latest .NET Framework, here it is the .NET Framework 4.6 Features, click **Next**.



Follow the rest of the wizard's steps until the install is completed. Once .NET 4.6 or greater framework is installed on your server, then run the pre-requisites check again.

IIS not Installated

Don't have IIS installed yet? This is what you will see:



To Resolve:

Click the **Fix Issues** button on the Delinea Installer. Then run the pre-requisites checks again.

HTTPS Binding Error

Did you encounter an HTTPS Binding Error? Does it not clear after using the **Fix Issues** button?

To Resolve:

Close and re-open the Delinea Installer and run the pre-requisites checks again.

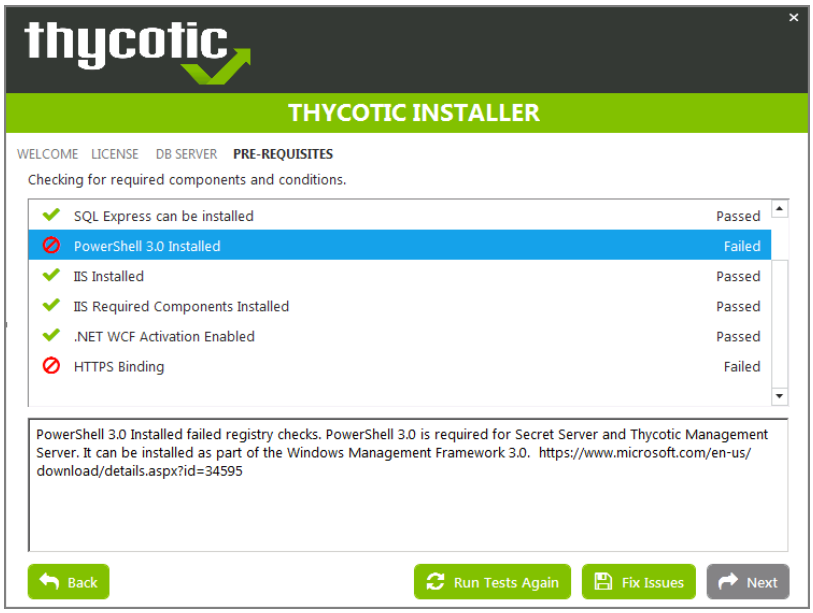
If the Binding error persists, verify the following:

For combined Privilege Manager and Secret Server installations, did you previously move the Secret Server app pool in IIS to its own website, rather than allowing it to reside under the Default website? see this KB for details.

The installer checks the Default Web Site for an HTTPS binding, and whether there is a certificate assigned to it. This means that if you pre-created the Secret Server Web Application and assigned the HTTPS binding to that site, you may need to manually move your previously installed Secret Server IIS site to reside back under the Default Web Site in IIS when installing Privilege Manager.

PowerShell Error

Are you receiving a PowerShell error? You may be trying to install Privilege Manager on an outdated server! Here's what you will see:



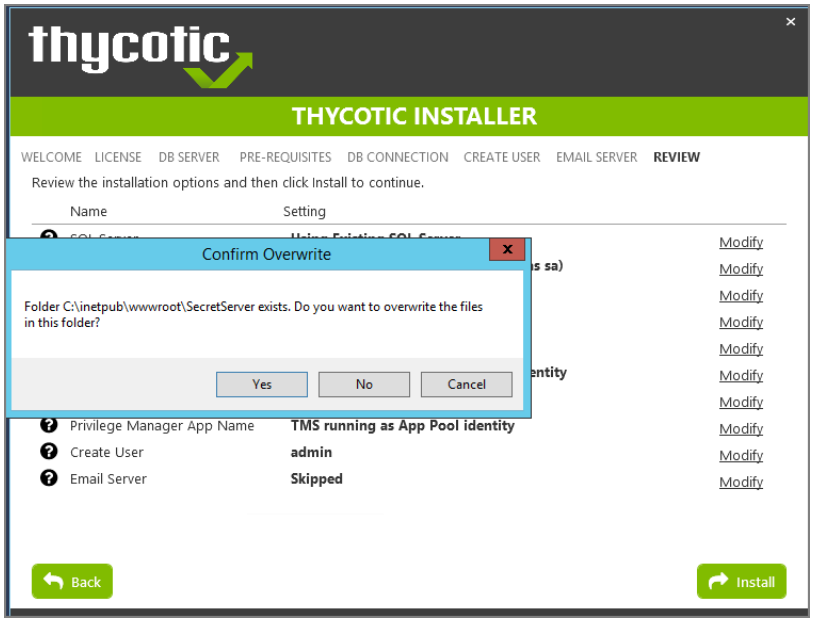
To Resolve:

You may need to update the server you are installing on. Please see our System Requirements Guide for supported servers. You can also manually download PowerShell 3.0 and install it from Microsoft's website here.

Once PowerShell is properly installed on your server run the prerequisites checks again.

Secret Server and Privilege Manager Installed

Already have Secret Server installed on your server? Here is what you will see:



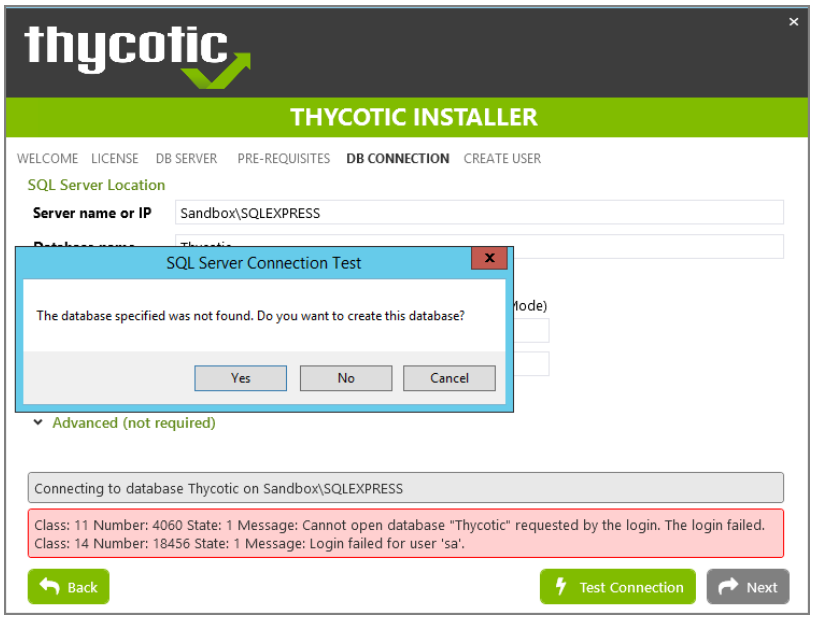
To Resolve:

We recommend installing new instances of Secret Server and Privilege Manager on a clean server.

If you do not already have an instance of Secret Serveror Privilege Manager on this server to your knowledge, these files may exist due to an incomplete install. Check with anyone with access to this server who may have attempted this install previously. Only if you are confident that this is your first and only existing Secret Server or Privilege Manager instance click **Yes** to overwrite the existing files.

Error in DB File Path

Trying to test your connection to an existing SQL database? Here's what you will see:



To Resolve:

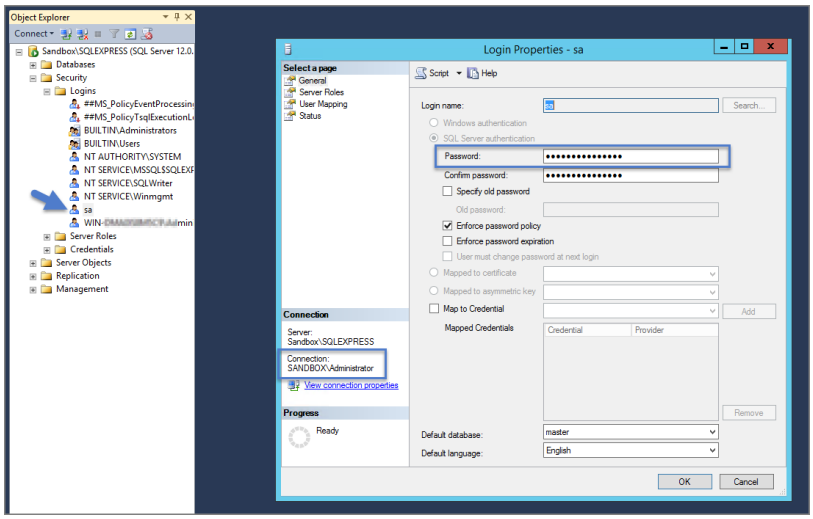
This message means that your file path to your database is incorrect or your account does not have the correct permissions to access it.

If you have an existing database,

1. Navigate to your SQL Server Management Studio and log in.
2. Navigate to **Security** | **Logins** and right click on the account you are using for your Delinea product, click **Properties**.

The information you need to enter in the Delinea Installer for the connection path is listed in the bottom left corner under Connection. You will also need to provide this account's password.

Note: This account must have **db_creator** permissions.



Outdated Browser

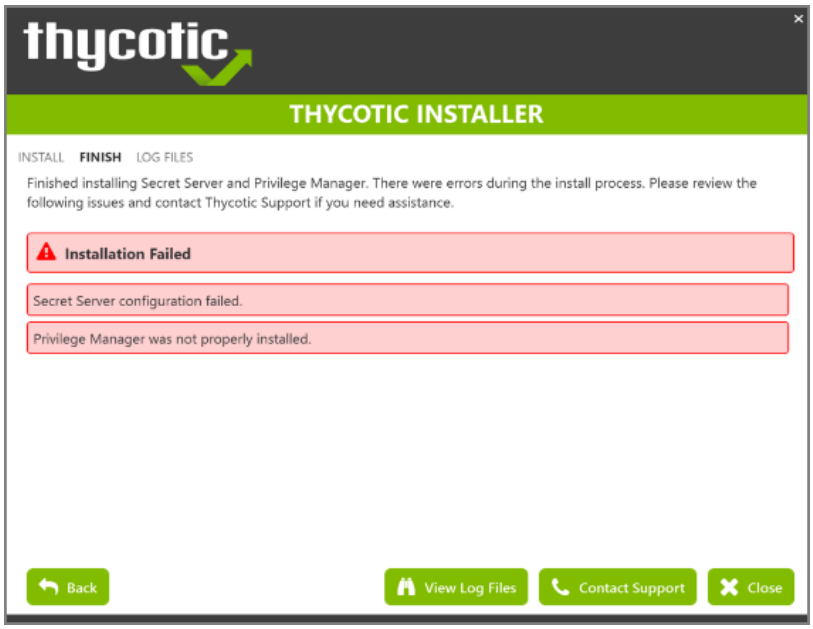
Are you trying to open your newly installed Privilege Manager in an outdated version of Internet Explorer? Here's what you will see:

To Resolve:

Try opening Privilege Manager in a different browser, or update your Internet Explorer browser.

Integrated Authentication Error

Are you using Integrated Authentication and your installation failed? Here's what you will see:



To Resolve:

For clients using Windows Integrated Authentication, the Delinea installer does not validate your database connection, so entering the wrong database server, database name, or if the user account provided does not have access to the database, your install will fail without warning you in advance. To resolve, please verify your database connection settings and enter them correctly under the **DB Connection** tab during the installation process.

Privilege Manager Logs

The following topics dealing with logs in Privilege Manager are available:

- Where are My Server Logs?
- Where are My Agent Logs?
- SQL Server Transaction Logs
- User Interface and Ports

SQL Server Transaction Log

SQL Server maintains a history of all operations using a Transaction Log. If this transaction log becomes full, you may receive one or more of the following errors:

- System.ArgumentException: Cannot add two background tasks with the same name.
- Thycotic.Data.DataAccessorException: The transaction log for database '{database}' is full. To find out why space in the log cannot be reused, see the log_reuse_wait_desc column in sys.databases

By default, a transaction log can grow to an unrestricted size. A transaction log may become full under the following circumstances:

- The drive where the transaction log file is kept is out of disk space.
- The transaction log file hits its growth limit.

Possible solutions include:

- Backing up the log.
- Freeing disk space so that the log can automatically grow.
- Moving the log file to a disk drive with sufficient space.
- Increasing the size of a log file.
- Adding a log file on a different disk.
- Completing or killing a long-running transaction.
- Switching to simple recovery mode and truncating the log.

For more detailed information on transaction logs in SQL, see http://technet.microsoft.com/en-us/library/ms345583%28v=sql.90%29.aspx

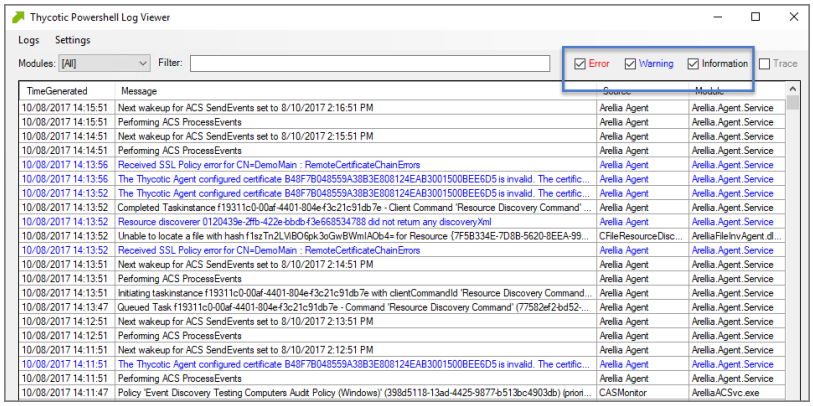
Where are My Agent Logs

If something is going wrong on specific endpoints, another place to look for answers is in your agent's Event Log Viewer.

In your endpoint machine, navigate to your Delinea Agent files. This is usually located in `C:\Program Files\Thycotic\Powershell\Arellia.Agent`. Right-click on AgentLogViewer and select Run with Powershell. This will open your Agent Event Log Viewer, which shows updates in real time as the agent communicates with the Privilege Manager server.

For remote access, Agent logs are also viewable through the Windows Event Viewer.

Scroll all the way to the top of the page to see the most recent activity from your Delinea Agent. Uncheck the Information box on the upper right-hand corner to narrow search results for any Errors and Warning messages that may be occurring. You can also double-click any line item for more detailed information about each event.



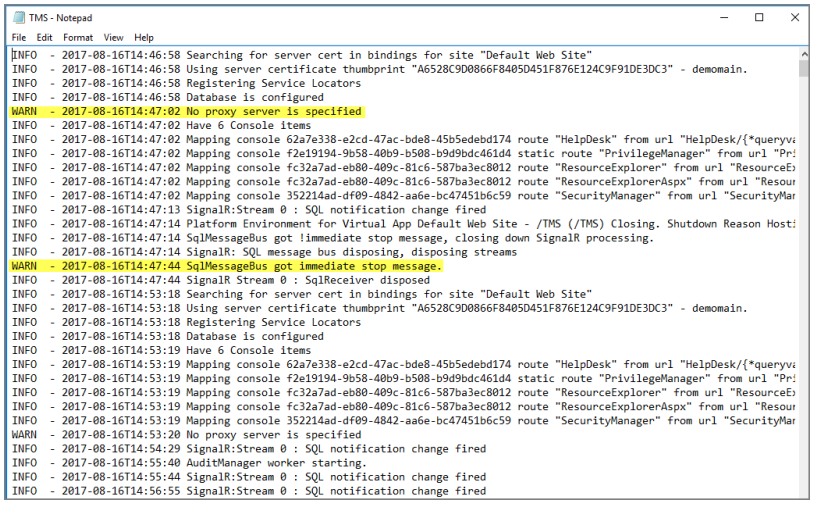
Where are My Server Logs

When something goes wrong in any technological platform, the best clues about 'why' are usually buried in log files. In Privilege Manager, it depends on 'what' is happening to know where to look for clues first, but server log files are usually a good are to start.

All Server-Side Privilege Manager Logs are written to `%PROGRAMDATA%\Thycotic\Logs`. Usually that means the folder path on your server is `C:\ProgramData\Thycotic\Logs`.

Keep in mind that the shared folder ProgramData can be hidden. You can enter this path directly in your file explorer's navigation bar to find the logs.

Within the Logs folder, you will find one log file for each web app. (e.g. Tms.log, Tms-Setup.log, Tms-Worker.log, etc.). When submitting a case to Delinea's Support team, it is always a good practice to send these log files.



By default, these log files will contain informational events, warnings, and errors.

Not included in your default logs are verbose/trace/debug errors, but this is configurable via the web-logging.config file in each web app directory discussed below. If interested in changing your log settings, you can find more information about the Log4Net Core “Level Value” options here: https://logging.apache.org/log4net/log4net-1.2.11/release/sdk/log4net.Core.Level.html

To edit log settings (i.e., log trimming by size, type of recorded Log4Net Events) you can edit the code in your web-logging file, usually located in `C:\inetpub\wwwroot\TMS\web-logging`. By default, this file looks like this:

```
<?xml version="1.0" encoding="utf-8" ?>
<log4net>
<root>
<level value="INFO" />
<appender-ref ref="Thycotic.LogFileAppender" />
</root>
<logger name="Thycotic">
<level value="INFO" />
</logger>
<appender name="Thycotic.LogFileAppender" type="log4net.Appender.RollingFileAppender">
```

```
<file value="${ProgramData}\Thycotic\Logs\TMS.log" />
<rollingStyle value="Size" />
<maxSizeRollBackups value="34" />
<maximumFileSize value="1MB" />
<lockingModel type="log4net.Appender.FileAppender+MinimalLock" />
<layout type="Thycotic.Platform.Logging.Log4NetSimpleLayout,Thycotic.Platform"></layout>
</appender>
</log4net>
```

User Interface and Ports

When something goes wrong in Privilege Manager, the UI has a few places worth checking:

- **Admin | Diagnostics** - this will give you information on Agents and Operating Systems, click **Console Logs** for more details.
- **Reports | Diagnostics** – A great place to look for some useful programmed reports on Agents, Remote Tasks, Policies Not Received by Agents, Summary of Gauge States, and Licensing.

Connectivity

Are you having Connectivity issues? A few things to keep in mind:

- Outbound access from the agent to the server is done by default over port 443 (the standard port for HTTPS communication), but you may specify a different port if desired.
- The only port that the agent listens on is port 5593. This is not required. For example, you can block this port and agents will pull from the server on a set schedule.

Performance Issues

This section provides a collection of possible performance issues and their remediation options.

The following topics are available:

- Improve Boot-up Performance
- Unable to access Privilege Manager
- Factors affecting Compilation Times are discussed as best practice.

Increase Boot-up Performance

In environments with policies having many filters, starting policy analysis during boot-up can impact the overall boot performance.

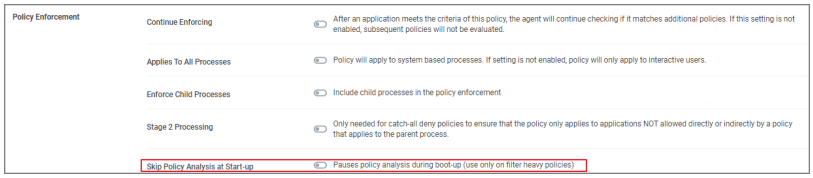
If this is an issue in your environment you can pause the policy analysis during boot. Pause analysis during the boot-phase decreases CPU utilization and delays to the boot process.

The end of the boot-phase in which policy analysis is paused, is defined as the CPU utilization after start-up being below 25% for a minimum of 120 seconds. Once that benchmark is reached, policy analysis will start.

Warning: Using this feature opens your systems up to vulnerabilities during the boot-phase due to policies not being enforced for a certain amount of time, until the above mentioned condition is met.

Enable Pausing Policy Analysis during Boot-up

Each policy by default has a list of policy enforcement options under **Advanced | Policy Enforcement**.



To enable pausing policy analysis during boot-up on filter-rich policies, set the **Pause Policy Analysis During Boot** switch to on and save the change.

Endpoint Performance

Generally speaking, "Installing Windows Agents" on page 69 have a small footprint on endpoint machines. Memory usage, CPU usage, and boot time should be negligibly impacted. If certain best practices are not followed, endpoint performance can be affected.

Item to Consider

Troubleshooting items to consider if endpoint performance issues are reported include the following.

Anti-Virus

Ensure anti-virus exclusions are in place for all anti-virus products in the environment. Refer to "Antivirus Exclusions" on page 56.

Secondry File Hash Exclusions

Ensure secondary file hash exclusions are in place. Refer to "Exclude File Extensions during File Hashing" on page 810.

These are usually helpful for developers running compilers or opening 1 TB database files. It may not affect boot-up items, but should be part of resolutions for some endpoint performance complaints.

No Application Control Policies have **Applies To All Processes** enabled in the Advanced Settings. This should be used very sparingly, as it will target non-interactive processes (including system processes) and cause more processing time. This is only used in the rare instance that it is required. This is needed to target a file that appears in the Agent logs like this:

```
DoProcessWork Ignoring Process 42576 (C:\Windows\System32\sppsvc.exe) as it is a protected process
```

Checking **Applies To All Processes** will allow the policy to target this file. It should only be needed in very few, rare instances. By default, this should be unchecked, unless absolutely necessary.

Policy Enforcement

Most policies do not have **Continue Enforcing Policies** and **Continue Enforcing Policies for Child Processes** enabled in the Advanced Settings. These options are typically disabled for most policies. With the options disabled, a target application is caught by a policy, performs the **Actions** on the policy, and then processing completes. With these enabled, a target application is caught by a policy and processing continues against other policies, which is not the way an efficient policy stack is created.

Consider enabling **Skip Policy Analysis at Start-up** in the Advanced settings on some Policies. Refer to "Increase Boot-up Performance" on page 932

If this is checked on a Policy, it will pause that Policy's analysis during boot-up. Understand the risk associated with this and consider enabling it on Policies that should not be targeting boot-up files.

Present in Signed Security Catalog

The Application filter for **Present in Signed Security Catalog** should be used as an Exception filter in some policies, especially Block policies. This filter dynamically targets the files that are deployed via the Operating System (OS). That includes a lot of files that run at boot-up.

Make sure that Block policies have this filter as an Exclusion filter, so that OS files are not inadvertently blocked. You may want to create a policy with a low policy priority number that allowed the **Present in Signed Security Catalog** to run in standard context. This allows quick processing in the stack without elevating or blocking them. If an Allow policy for **Present in Signed Security Catalog** is used to elevate those files, the Elevation policy would need to occur before the Allow policy.

Audit Policy Events

Make sure that **Audit Policy Events** are not enabled on many of your policies. This creates more work for the endpoint and should definitely not be enabled on every policy. This should only be on Discovery policies and there should be some self-imposed limitations on using it. If this and **Continue Enforcing Policies** are enabled on multiple policies, the same file event can be caught by multiple policies (adding to process) and feedback of the event can be gathered multiple times (very inefficient).

Policy Filters

Application Control policies should not have more than 100 total filters on the policy. The combined number of Application filters, Inclusion filters and Exclusion filters should not exceed 100. Processing time of the agent is more efficient with two policies of 100 filters vs. a single policy with 200 filters. Review the Application Control policies to determine the total number of filters per policy.

Summary

If endpoint performance issues are reported by a subset of users, determine if there is commonality in the roles of the effected users. For example, if the effected users are developers, review the suggestions above and make sure that "Secondry File Hash Exclusions" on the previous page are addressed.

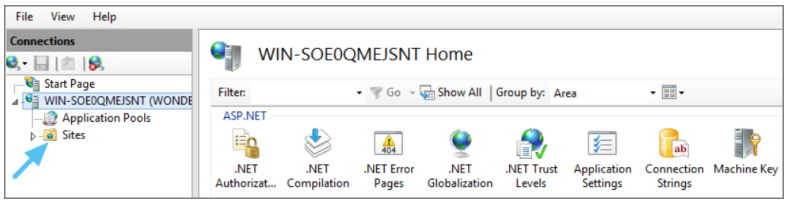
Additionally, understand the types of Application Control policies that are used in the environment. Are Application Control policies mainly focused on Elevation policies to remove Admin rights? Or, is a set of strict Allow / Block policies enabled to restrict allow all files that need to run? If strict Allow / Block policies are in place, investigate ways to simplify the filters used to target applications. For example, instead of creating individual Application filters for files in `C:\Windows`, target by the file location since standard users (without Admin rights) do not have write access to that directory. Using one filter to target a large repository of files will be much more efficient than targeting each individual file separately.

Unable to Access Privilege Manager

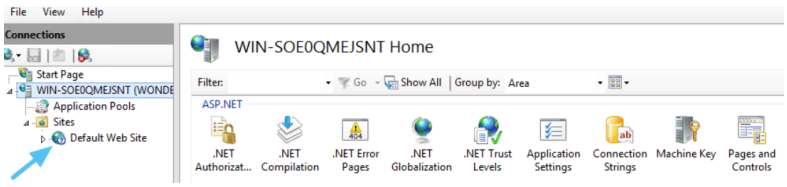
When attempting to login to Privilege Manager and you are unable to access the application window and you are continuously redirected to the login modal, verifying the IIS settings and resetting the app server might help.

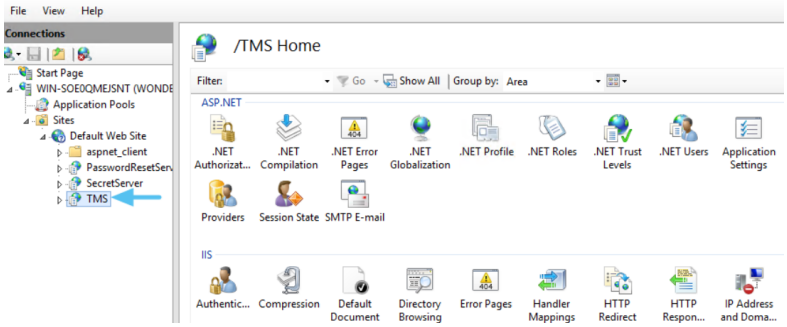
Resolve

1. Open **Internet Information Services (IIS) Manager**.
2. Expand **Sites**.

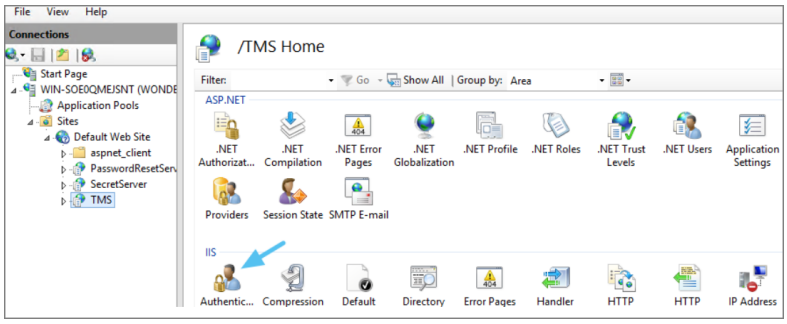


3. Click the **TMS** Site.

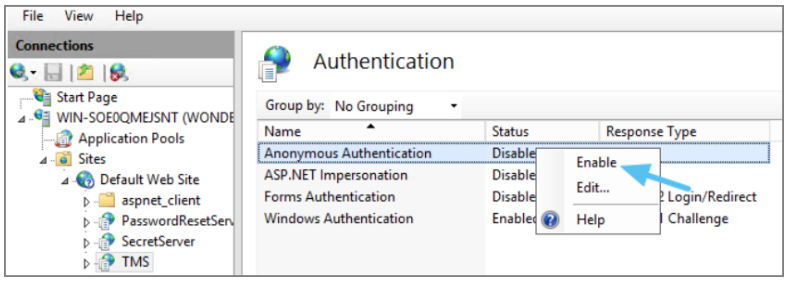




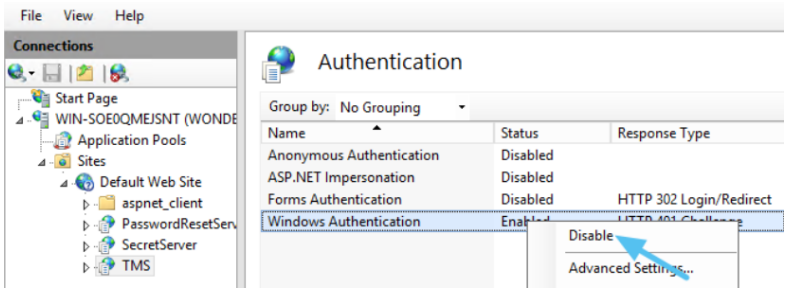
4. Click on **Authentication**.



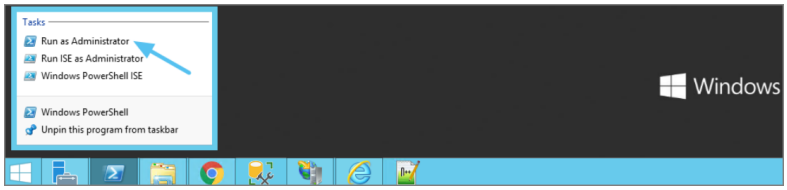
5. Right-click on **Anonymous Authentication**.
6. Click **Enable**.



7. Right-click on **Windows Authentication**.
8. Click on **Disable**.



9. Open **Powershell**, type `iisreset` and press **Enter**.



10. Launch Privilege Manager.

Troubleshoot with Tools

Using certain tools for troubleshooting purposes can help locating issues and finding a solution to a problem.

The following troubleshooting tools topics are available in this section:

- How to use the Thycotic Monitor for Troubleshooting
- Using Process Hacker for Troubleshooting
- Troubleshooting a Policy with Process Explorer

Using Process Explorer for Troubleshooting a Policy

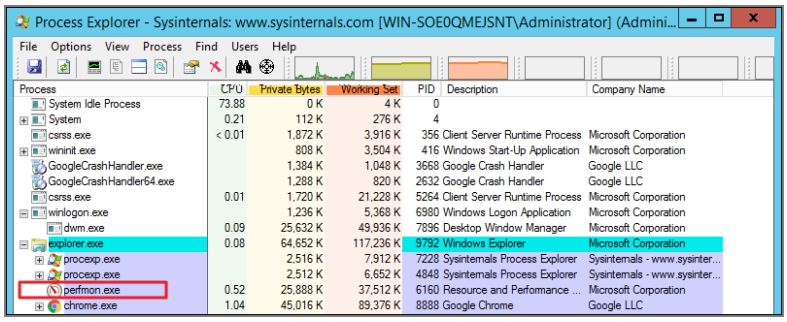
This topic describes how to troubleshoot a policy with Process Explorer. Process Explorer is used to look at policies that grant administrative privileges, but don't seem to work when:

- an application is accessed, or
- actions are supposed to run.

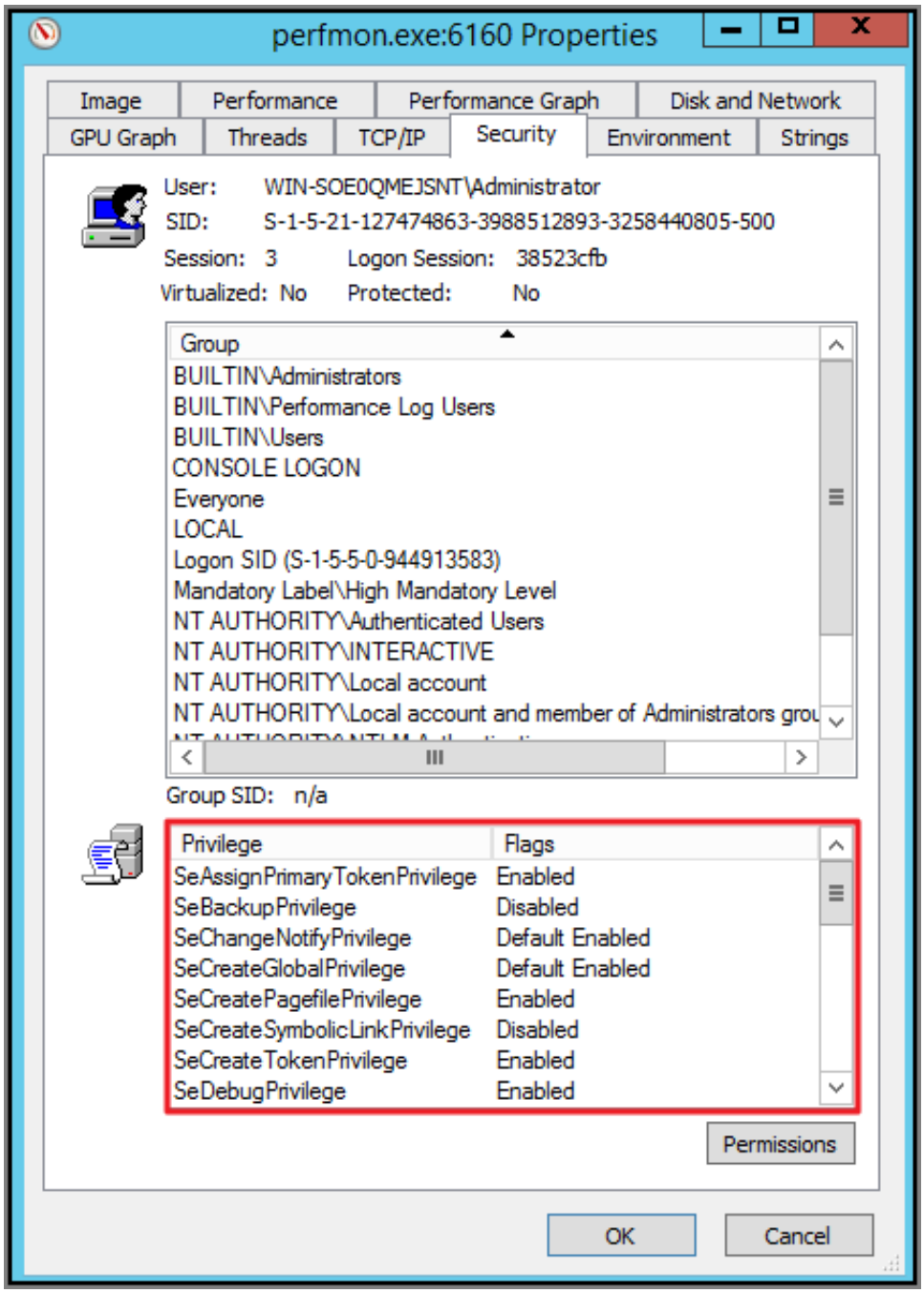
In the example below, the policy allows resource monitor to run but the application is blank due to not having sufficient Windows Privileges. You can use Process Explorer to determine the correct Windows Privileges to add to the policy in order to use the resource monitor application.

Detailed Troubleshooting Steps

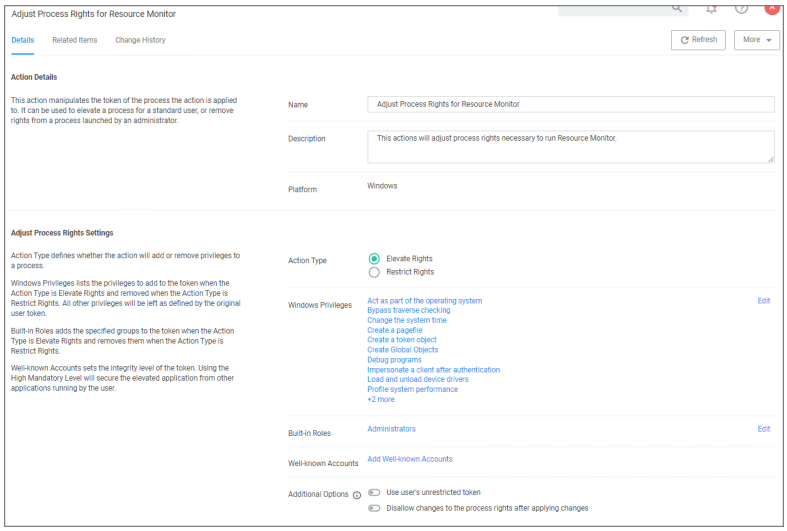
1. Download Process Explorer from the Mircosoft website and extract the downloaded ProcessExplorer.zip file locally on your system.
2. Open **Process Explorer**.
3. Next open **Resource Monitor** as the Administrator.
4. Navigate back to the Process Explorer Window and find the Resource Monitor application (perfmon.exe).



5. Right-click and select **Properties**.
6. Select the **Security** tab.
7. Under the Privilege section, you can see all the flags that are enabled in order to use the application.



8. Launch Privilege Manager and navigate to **Admin | Application Policies**.
9. Select the policy that elevates privileges to run **Resource Monitor**.
10. Under **Adjust Process Rights**, modify settings.



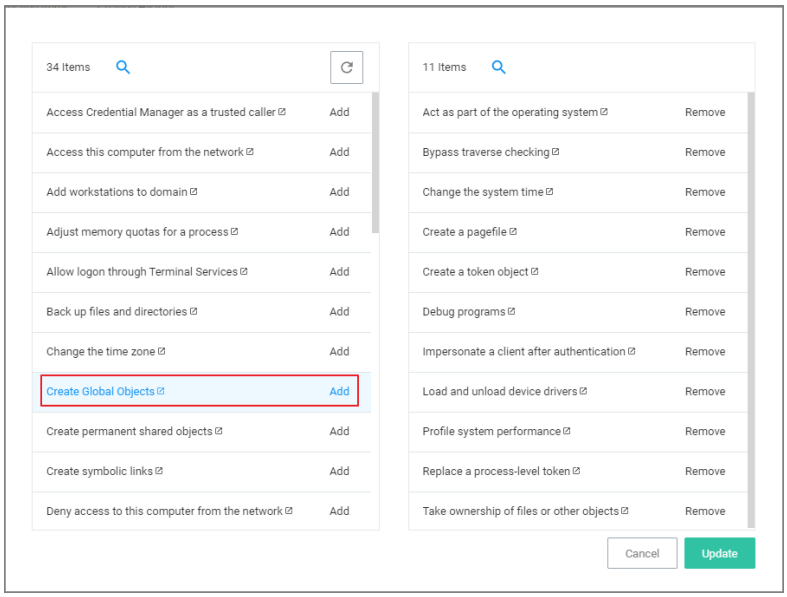
a. Select **Add Administrative Rights** or the elevation action you are using.

11. Under **Windows Privileges**, click **Edit**. (For this step you will have to determine which flags are enabled in Process Explorer in order to add the additional Windows Privileges to the action.)

12. In another window, navigate to the following Microsoft web site @ https://docs.microsoft.com/en-us/windows/win32/secauthz/privilege-constants. The site will show the name of the Windows Privileges, along with the user right information that needs to be added to the action in Privilege Manager.

    For Example: The privileges listed under the properties security tab show **SeCreateGlobalPrivilege** as enabled. On the Microsoft website for Privilege Constants @ https://docs.microsoft.com/en-us/windows/win32/secauthz/privilege-constants, the user right for SeCreateGlobalPrivilege privilege is: **Create global Objects**.

13. Enter the user into the search box and then select the user from the returned list. In this example, enter in **Create Global Objects**.



14. Click **Add**.
15. Remove any actions you don't need.
16. Click **Update**.
17. Click **Save Changes**.

Once the agent has received the updated policy, the additional Windows Privileges will be applied to the application next time it is launched.

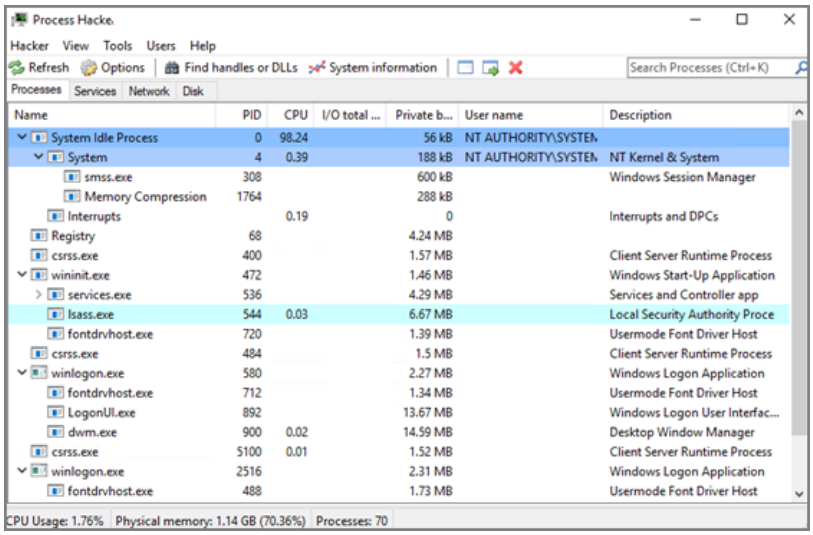
Using Process Hacker for Troubleshooting

Process Hacker is a third-party tool that can be useful for troubleshooting as well.

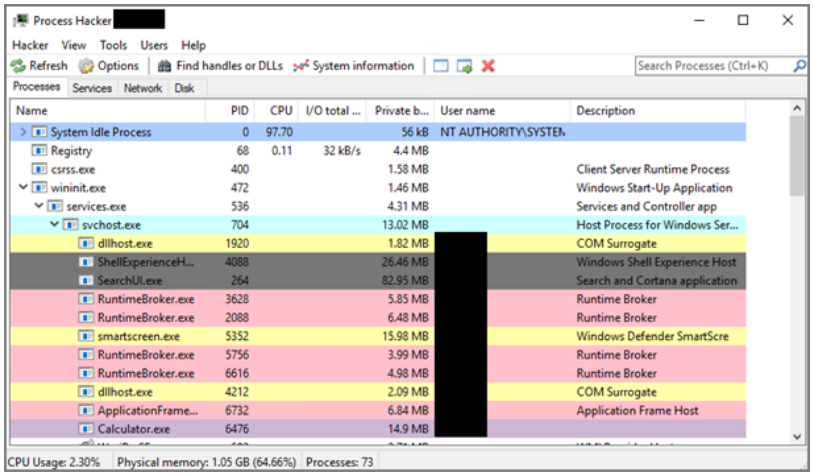
> **Note:** Since this is a third-party tool, Delinea is not responsible for any part of the application and has no control over it.

Process Hacker can be used to determine whether a process you are trying to apply an action to is a parent process or a child process of another application. If you do not want to install Process Hacker on the endpoint you are troubleshooting from, there is a portable version available as well that does not require it to be installed on the machine.

When you open Process Hacker, you will notice a screen like the one below that shows the running processes on the machine.

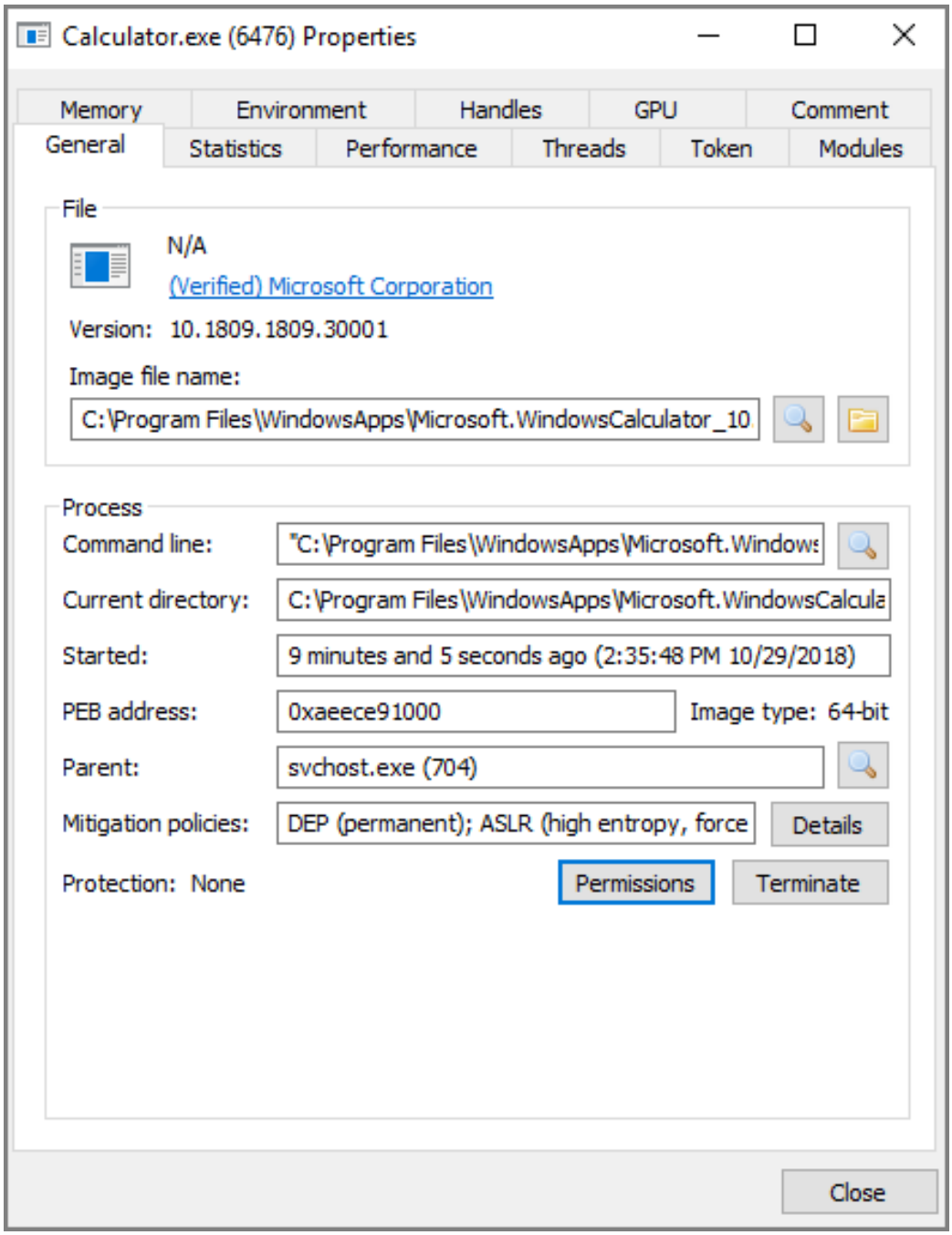


You will notice that some processes are listed below other processes. The processes listed under other processes are child processes of the top parent process. For example, after opening the Calculator app on a test machine, the Process Hacker window looked like the screen shot below.



You can see at the bottom of the screenshot above that the Calculator.exe process is actually a child process of the svchost.exe process, which itself is a child process of the services.exe process, which is a child process of the wininit.exe process. Not all processes will be nested underneath as many parent processes as in this example.

You can also double-click on the process to open a window with more information about the process. You can find the parent process that way as well on the **General** tab of that window. The screen shot below is what the **General** tab shows for the Calculator.exe process.



You can see the Parent field, which shows you that the svchost.exe process is the parent of the Calculator.exe process. If you are viewing the parent process, then in the Parent field you will see *Non-existent process* instead of seeing a parent process listed.

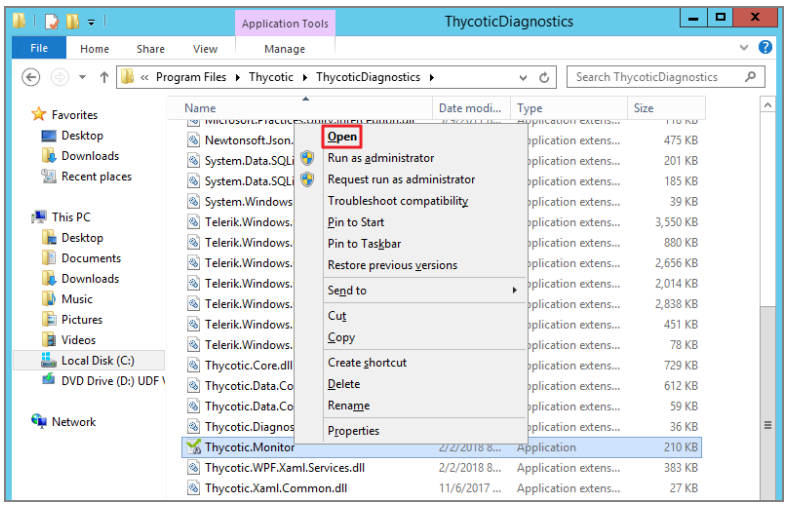
You will also notice a **Token** tab in the screenshot above. That tab is useful in showing you whether the process is running elevated; it shows an **Elevated** field, with values **Yes** or **No**. It will also show you the process security tokens that the application needs to run. You normally do not need that information, but it is good to know where to find it, just in case.

As you can see from the information above, Process Hacker is a third-party tool that can be useful when troubleshooting why a policy is not applying like you think it should. For example, if you are trying to elevate a specific application or process, it might not be working correctly if that process is actually a child process. In that case, you can configure the policy to target the parent process and apply that same action to the child processes. You might not need to target the parent process in all situations, but sometimes it will be necessary.

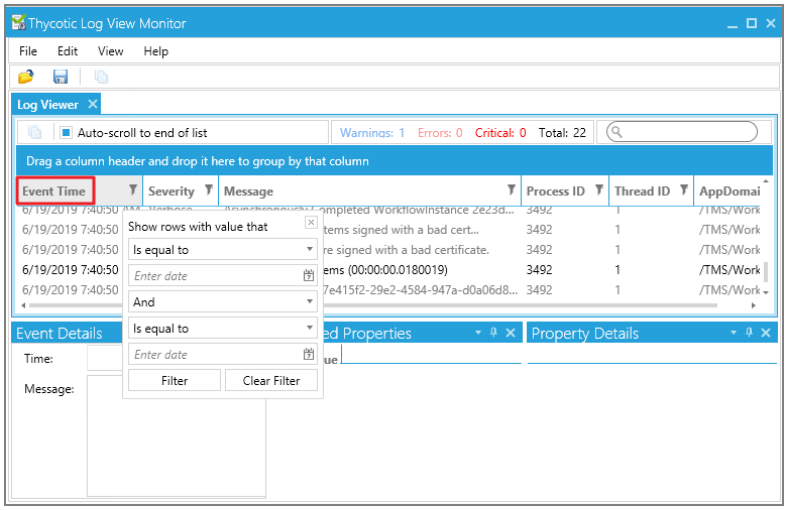
Using Thycotic Monitor

While using Privilege Manager, you can utilize the Thycotic Monitor to help troubleshoot issues that occur on the web console.

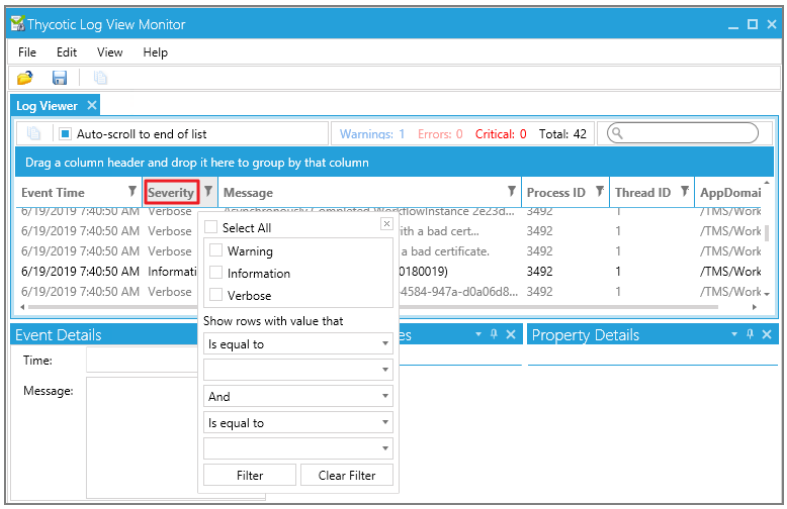
1. On the server with the Privilege Manager installation navigate to `C:\ProgramFiles\Thycotic\ThycoticDiagnostics` and open the Thycotic Monitor.
2. Right-click **Thycotic Monitor** and select **Open**.



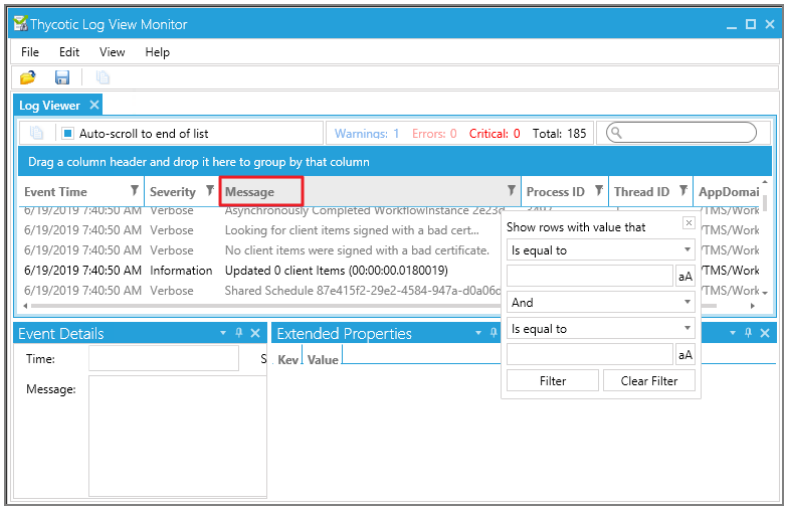
3. Left-click the filter icon for **Event Time** to filter for specific times in order to better help find a specific event.



4. Left-click the filter icon to access **Severity** settings and filter for specific severity levels.



5. Left-click on the filter icon for **Message** to narrow down specific messages and GUIDs to help find errors.



Note: If you're attempting to troubleshoot an issue open the Thycotic Monitor and replicate the issue on the server where Privilege Manager is installed. It may also be helpful to grab a screen shot, including a time-stamp from when you replicate the error. This will help with troubleshooting.

1. Open the Thycotic Monitor.
2. Replicate the issue server-side.
3. Select **File**.
4. Select **Save**.

The file saves as a .tracelog file type. You can upload the tracelog to your support case or review the event details for further information.

Release Notes

This section includes the most recent Privilege Manager Release Notes.

- "12.0.0 Release Notes" below

Previous versions:

12.0.0 Release Notes

Release Schedule

Privilege Manager Cloud Release – March 30, 2024

Privilege Manager On-Premise Release - April 12, 2024

Windows Agent Software

12.0.1016 Bundles Privilege Manager Agent Installer

12.0.1016 Core Thycotic Agent (x64)

12.0.1016 Core Thycotic Agent (x86)

12.0.1016 Application Control Agent (x64)

12.0.1016 Application Control Agent (x86)

12.0.1016 Local Security Solution Agent (x64)

12.0.1016 Local Security Solution Agent (x86)

12.0.1016 Bundled Privilege Manager Core and Directory Services Agent

12.0.1002 Directory Services Agent (x64)

macOS Agent

12.0.0.058 Privilege Manager macOS Agent (Catalina and later)

When upgrading Privilege Manager to a newer version, Delinea recommends upgrading the Directory Services agent such that both are running on the same release version.
Privilege Manager exclusively supports operating systems (OS) that have not reached their official End of Support. For optimal performance and compatibility, it is recommended to utilize Privilege Manager on a supported and actively maintained OS.
Delinea recommends as a best practice to create system restore points prior to doing system changes such as patches.

Important: Delinea supports the use of software versions up to a year prior to the current version. The links to prior versions are found in the PDFs available for prior versions on Links to Previous Versions.

Stability and Reliability Improvements

As part of our continuous efforts to enhance our software, we are pleased to introduce key improvements in the stability and reliability of the Privilege Manager in our latest release. These updates significantly contribute to a more stable and reliable experience for all our users.

Scheduled Agent Jobs Optimization

Improvement Detail: Users may notice refined scheduling of Privilege Manager's scheduled agent jobs. These changes aim to boost the system's overall reliability and performance. The change was applied to a subset of customer environments initially, and is now rolled out to all environments with the 12.0.0 release.

New Policy Introduction: The **Task Scheduler - Ensure Randomness** policy has been integrated to improve how agents execute scheduled jobs. It ensures adherence to the random delays predefined in those jobs, enhancing task execution efficiency.

Certificate Validation for SSPM Agents

For both the Windows Agent and macOS Agent, by default, validate server certificate is turned off. However, if your server domain includes one of these, then validate server certificate will automatically be turned on and the server certificate will be validated:

- .privilegemanagercloud.com
- .privilegemanagercloud.eu
- .privilegemanagercloud.com.au
- .privilegemanagercloud.com.sg
- .privilegemanagercloud.ca

To force this setting to be enabled for use with an on-premise Privilege Manager server via MDM deployment of the agent, refer to the documentation:

Installing Windows Agents

Installing macOS Agents

Using regex with Group Memberships

With the ability to be able to use regex (preferred) or wildcard values in the local group membership controls in 11.4.3, you must use specific and restrictive regex. We cannot guarantee that your expression will never include an unintended user. Please validate the expression yourself with one of the many online regex testers, and check group members regularly.

Jamf Pro Classic API: Basic Authentication Removal

Jamf has announced that the Classic API will no longer be enabled by default for new Jamf Pro instances for enhanced security. Support for Basic authentication is scheduled to be removed on March 31, 2024.

Beginning with Privilege Manager 12.0, Delinea supports the Jamf Bearer Token Authentication method.

This requires updating the Privilege Manager credential that is used to connect to Jamf Pro. The instructions for this can be found in "Creating a Privilege Manager Credential" on page 636.

Service Process Update for LSA Privileges

The Thycotic Application Control service is no longer configured to use a virtual service account; it is now configured to run as NT AUTHORITY\SYSTEM (local system) again.

A different mechanism is now used to ensure that the service process has all of the Local Security Authority (LSA) privileges required for it to function properly. LSA privileges do not need to be explicitly granted for the service to run properly, and there is no need for GPOs (Group Policy Objects) to be created or modified as part of deploying the agent.

macOS 10.15 Catalina Support

Privilege Manager version 12.0.0 is the last version of the Mac agent to support macOS 10.15 Catalina, for which Apple has not released a security update since July 2022. Going forward,Privilege Manager will follow the common practice of supporting those OS versions that Apple itself supports with security updates, namely, the current and

two previous versions of macOS. (We anticipate discontinuing support for macOS 11 Big Sur when we implement support for the next release of macOS in late 2024.) We encourage our users to upgrade to a supported version of macOS to continue receiving the latest features and security updates.

Software like Privilege Manager is more closely coupled to the lower-level macOS frameworks than other applications; in particular, the security frameworks show a faster pace of evolution as Apple continues to update macOS. Adopting this support policy enables us to better follow Apple's guidance by using the latest and most secure technologies, rather than relying on outdated or even deprecated frameworks. In this way, we can provide our customers with a better user experience and improved application functionality.

Enhancements

- A new Microsoft Entra ID Authentication action enables single or muli-factor authentication for Windows and macOS, using Microsoft Entra ID. Refer to "Microsoft Entra ID Authentication" on page 506.
- The default schedules for out-of-the box policies have been updated to help alleviate sudden spikes of traffic to the server.
- When creating a new Email Approval Process task, the UI has been changed slightly to allow the URL to be included in the tasks XML, without having to save the task first.
- Creating a new agent configuration for a macOS Computer Group now allows you to define a unique secure token credential for that group. Previously, only a single credential could be defined that would be shared by all configurations.
- Improvements have been made to the Managed Group UI experience improving speed and reliability of the information displayed. Delinea recommends adding Built-in users to the managed group using the Local Users option only.
- The **Policy Name** field is editable in the policy view, so users no longer have to use the **Rename** option.
- The message informing users that there is too much data in a report to export to a PDF has been enhanced.
- Active Directory sync performance has been enhanced to limit the frequency of the full AD import to once every 24 hours. Also, a new facility allows customers to only enter the names of the AD Groups that need to be imported. Delinea recommend that customers only import the resources that they actually require, that the new Groups functionality will allow.
- A new task has been created to remove resources, based on the last modified date. The resources available to be deleted are Computers, Files, Domain Users and Domain Groups. The job is accessed via the Resources folder. Refer to "Resource Cleanup" on page 784.
- Two reports, available in Application Control, provide details of the policies and policy filters configured in a Computer Group. Refer to "Policy Modifications Reports" on page 895.
- A new **Skip To** link has been added to the top of the left hand navigation panel for accessibility purposes. In the absence of keyboard focus, pressing Tab gives users the option to shift the focus to the main area of the screen, or remain in the navigation panel.
- A new feature for **Export** is available on the Application Policies page, allowing the selection of multiple policies that can be exported to a ZIP file and imported elsewhere. See "Exporting Policies" on page 435.

Bug Fixes

- An issue with exporting and importing hash based filters has been fixed.
- The All Unclassified Applications filter is not easily maintained and largely unused. It will be deleted during upgrade, unless it's being actively used in a policy.
- The Summary of Application Approvals and Denials report and its drill-down have been fixed to improve performance and should no longer show duplicate rows.
- Fixed an issue where users and groups with a space in the account name (not display name) were not being imported properly.
- This release fixes performance issues from high SQL worker utilization caused by stored procedures that run as part of the collection and resource targeting updates.
- The Command Line Approval Request Action was updated to be included as part of the macOS actions, along with removing redundant text.
- An issue was resolved where copying a JIT policy and making any edits to the policy would result in the **Action** of the policy being changed from **JIT Elevation** to something else (e.g., **Block**, or **Elevate**). Now, all policies with a JIT **Action** will display **JIT Elevation** when they are edited.
- The banner "Attention: There are 2 or more critical alerts that require action" can now be closed when clicked.
- An update made increases the time it takes to retry registering an invalid agent.

Agent Specific

Windows

- A problem was fixed where the Restrict File dialogs action was not detecting the display of an Open/Save file dialog in Microsoft Office applications such as Excel. Another problem was fixed where context menus could be erroneously re-enabled in a file Save As dialog, even though the Restrict File dialogs action had been applied to it.
- A problem where enforcement of a managed group policy for the BUILTIN\Administrators group would fail under a specific set of conditions based on how the policy was configured has been resolved. Now, when those conditions are encountered, the operation is allowed to performed successfully after some internal corrective action is taken by the client-side code in the agent.
- A legacy component, no longer required to be present in the agent, was causing some applications to fail to run properly in rare situations, when a shell execute operation was performed. The legacy component has been removed to prevent the problem from occurring in the future.
- A update was made to the token elevation code to ensure that all groups related to full or partial administrative rights are now fully enabled when an elevated token is assigned to a process via an elevation policy. Previously, groups such as Domain Admins were being left disabled, even though BUILTIN\Administrators was being added to the token during elevation. The failure to properly re-enable disabled groups could result in an elevated process still failing access checks or failing to perform certain administrative operations.
- An issue was resolved where the Privilege Manager agent was unnecessarily applying a certificate filter to a secondary file, which in some cases could cause performance issues and cause files to be locked, specifically when opening large database files in MS Access.

macOS

- Addressed an issue where the Mac agent would sometimes try to register with an invalid agent ID (all zeroes). When installing the upgrade on agents in this state, it will be necessary to re-enter the install code.
- The macOS Agent now correctly elevates .pkg policies when a white space exists in the .pkg name.

Known Issues

- Adding a local users (Regex) definition to a managed group that will include built-in users, will result in displaying any built-in users under their own line in the Members table rather than the Regex line.
- Adding a manual users definition to a managed group that will match a built-in users, will result in displaying two lines for the same user. This can be simply resolved by removing the named user line and keeping the built-in user line.

11.4.3 Updated Release Notes: Thycotic Application Control (build 3225)

Important: Only 11.4.2 and 11.4.3 (original release / build 3220) have the Virtual Service Account requirements. Delinea strongly recommends upgrading directly to this 11.4.3 Update (build 3225) from 11.4.1 and earlier.

Release Schedule

Privilege Manager Cloud Release - Tuesday, February 21, 2024

Privilege Manager On-Premise Release - Tuesday, February 21, 2024

Windows Agent Software

11.4.3235 Bundled Privilege Manager Agent Installer
11.4.3235 Core Thycotic Agent (x64)
11.4.3235 Core Thycotic Agent (x86)
11.4.3235 Application Control Agent (x64)
11.4.3235 Application Control Agent (x86)
11.4.3235 Local Security Solution Agent (x64)
11.4.3235 Local Security Solution Agent (x86)
11.4.3235 Bundled Privilege Manager Core and Directory Services Agent
11.4.3032 Directory Services Agent (x64)

macOS Agent

11.4.3.033 Privilege Manager macOS Agent (Catalina and later)
10.8.27 Privilege Manager macOS Agent (Catalina and previous)

When upgrading Privilege Manager to a newer version, Delinea recommends upgrading the Directory Services agent such that both are running on the same release version.
Privilege Manager exclusively supports operating systems (OS) that have not reached their official End of Support. For optimal performance and compatibility, it is recommended to utilize Privilege Manager on a supported and actively maintained OS.
Delinea recommends as a best practice to create system restore points prior to doing system changes such as patches.

Service Process Update for LSA Privileges

The Thycotic Application Control service is no longer configured to use a virtual service account; it is now configured to run as NT AUTHORITY\SYSTEM (local system) again.

A different mechanism is now used to ensure that the service process has all of the Local Security Authority (LSA) privileges required for it to function properly. LSA privileges do not need to be explicitly granted for the service to run properly, and there is zero need for GPOs (Group Policy Objects) to be created or modified as part of deploying the agent.

11.4.3 Release Notes

Release Schedule

Privilege Manager Cloud Release – December 9, 2023

Privilege Manager On-Premise Release - January 5, 2024

Windows Agent Software

- 11.4.3220 Bundled Privilege Manager Agent Installer
- 11.4.3220 Core Thycotic Agent (x64)
- 11.4.3220 Core Thycotic Agent (x86)
- 11.4.3220 Application Control Agent (x64)
- 11.4.3220 Application Control Agent (x86)
- 11.4.3220 Local Security Solution Agent (x64)
- 11.4.3220 Local Security Solution Agent (x86)
- 11.4.3220 Bundled Privilege Manager Core and Directory Services Agent
- 11.4.3031 Directory Services Agent (x64)

macOS Agent

11.4.3.033 Privilege Manager macOS Agent (Catalina and later)

10.8.27 Privilege Manager macOS Agent (Catalina and previous)

When upgrading Privilege Manager to a newer version, Delinea recommends upgrading the Directory Services agent such that both are running on the same release version.
Privilege Manager exclusively supports operating systems (OS) that have not reached their official End of Support. For optimal performance and compatibility, it is recommended to utilize Privilege Manager on a supported and actively maintained OS.
Delinea recommends as a best practice to create system restore points prior to doing system changes such as patches.

Stability and Reliability Improvements

As part of our continuous efforts to enhance our software, we are pleased to introduce key improvements in the stability and reliability of the Privilege Manager in our latest release. These updates significantly contribute to a more stable and reliable experience for all our users.

Scheduled Agent Jobs Optimization

Timeframe: January 13th - February 16th

Improvement Detail: Users may notice refined scheduling of Privilege Manager's scheduled agent jobs. These changes aim to boost the system's overall reliability and performance.

New Policy Introduction: The **Task Scheduler - Ensure Randomness** policy has been integrated to improve how agents execute scheduled jobs. It ensures adherence to the random delays predefined in those jobs, enhancing task execution efficiency.

Upgrading with Virtual Service Accounts

Starting with version 11.4.2, the **Thycotic Application Control** service is run using a virtual service account named **NT SERVICE\ArelliaACSvc** instead of **NT AUTHORITY\SYSTEM** (LocalSystem). Note that virtual service accounts really are "virtual" in that there isn't a user account being provisioned on the computer. These accounts have been a supported feature since the release of Windows 7 SP1.

By default, all virtual service accounts are members of the group **NT SERVICE\ALL SERVICES**, and Microsoft grants the **Log on as a service** log on right to that group when Windows is installed. If that log on right is revoked from that group, the service will not start.

Important: Before upgrading to version 11.4.2 or newer from version 11.4.1 & older, review this information completely and ensure that your runtime environment complies with the stated requirements. Failing to do so will result in the application control service failing to function properly.

Refer to "Virtual Service Accounts" on page 90 in Upgrades.

Certificate Validation for SSPM Agents

For both the Windows Agent and macOS Agent, by default, validate server certificate is turned off. However, if your server domain includes one of these, then validate server certificate will automatically be turned on and the server certificate will be validated:

- .privilegemanagercloud.com
- .privilegemanagercloud.eu

- .privilegemanagercloud.com.au
- .privilegemanagercloud.com.sg
- .privilegemanagercloud.ca

To force this setting to be enabled for use with an on-premise Privilege Manager server via MDM deployment of the agent, refer to:

Installing Windows Agents
Installing macOS Agents

Using regex with Group Memberships

With the ability to be able to use regex (preferred) or wildcard values in the local group membership controls in 11.4.3, you must use specific and restrictive regex. We cannot guarantee that your expression will never include an unintended user. Please validate the expression yourself with one of the many online regex testers, and check group members regularly.

Enhancements

- When agents are failing to register because they are unknown or have an invalid install code, an alert will be raised in Privilege Manager. The alert has a link to a report that shows key details such as name and source IP.

  Privilege Manager Admins should review the list of invalid registrations and determine whether the computer needs to have the agent re-registered, or removed completely. Refer to "Addressing Invalid Agent Registrations" on page 184.
- By default only commonly-used items will appear in global search results. A check box has been added to the UI to enable returning all results. Note that this will include items most users shouldn't modify without the assistance of support.
- A new Agent Summary by Version report has been added to Privilege Manager. This report can be found under the **Reports** | **Agent** section. The report will display agent versions, generated from the core agent component, separated by the operating system.

  When a row is selected from the Agent Summary by the Version, users will be presented with Managed Computers by Agent Version, which displays all agents running the same core agent component version.
- Added the ability to select multiple events on the "Policy Events" on page 465 screen and acknowledge them in bulk.
- The character limit for Windows Users and User Groups has been increased from 20 to 64, and on macOS from 20 to 128.
- The User Group Management page now shows only built-in and managed groups by default. A toggle has been added to the top of the page to show all inventoried groups, but may time out on very large groups.
- Improvement to the Windows Agent Utility, ensure consistency when using the Agent utility to invoke Register or Update options.
- Windows Agents now include their Azure Device ID as part of the standard agent registration process.
- In version 11.4.3, the shell script used to uninstall the Mac agent has been replaced with an Installer package to perform this operation.

- In version 11.4.3, resource discovery in the macOS agent will report Mach-O header info and digital signatures for executables built solely for Apple silicon. For universal applications, both slices (Apple and Intel) will be reported.
- A new bundled EXE Installer includes all Privilege Manager Agents for Windows machines (Core, ACS, LSS), replacing the three separate deployments previously required. You can use the bundled installer directly on individual endpoints for testing or for production environments in either 32-bit or 64-bit environments.
- A title bar now appears on workstation messaging dialogs that provides information for screen reader software.
- On Mac workstations, user accounts can now be created with a random password instead of a static one.

Bug Fixes

- Using the File Upload feature of the Privilege Manager UI (Console) to upload a file whose size is a multiple of 1048576 bytes no longer results in a Bad Request error.
- The SQL query for Group Management has been updated so that it no longer shows duplicates.

Agent Specific

Windows

- Fixed an issue where some programs were being falsely detected as system components, and didn't appear in the Remove Programs Utility.
- Previously, the **Parent is a High-Risk Application** filter, associated with the Delinea Policy Framework policy **Malware Attack Protection** contained an old version of the Microsoft Edge filter. An up to date filter has now been included, so LOLBAS attacks instigated from Microsoft Edge will now be recognized where this policy is active.
- When a COM or MSI elevation policy has a justify or approval action and that action is cancelled, the default UAC elevation/consent prompt will no longer be displayed.
- Authenticated Justification Message Actions are now properly handling groups marked as **Use for deny only**, which previously could result in the action incorrectly producing a success result when a failure result should have been produced.
- The Immediate File Inventory action has been fixed in this release. The purpose of the Immediate File Inventory action is to force an inventory of an executable as soon as a policy with this action is applies.

  Note: If required, we advise this is used in test environments, when the product is initially being set up. It is not designed to be used long term, in large environments, as it will create a extra load on servers with every computer reporting the same inventory.

- The issue where HTML messages appear twice for policies that target MMC snap-ins has been resolved. The message will only appear once when the policy is prompted. This fix also addressed issues that caused the **Failed to obtain long prefix path for** error message in the Agent logs.
- Applications no longer open behind other windows following user interaction with a XAML/HTML action.
- Performance improvements have been made on 12th and 13th generation Intel processors.

macOS

- Updates have been made to the configuration of policies when controlling the usage of sudo. See "Configuring Block sudo commands for non-admin group users" on page 390 for detailed information.
- For the MacOS Agent Privilege Manager Preference pane, the Policies Last Updated time is now updated when either `updateclientitems` (**CLI** or **Pref Pane** button) or the Update Applicable Policies (Mac OS) policy is executed (**CLI** or **Schedule**) where there has been an update made to a policy details from the Privilege Manager Server.

  Previously, invalid modifications to the Mac agent configuration policy could lead to various issues, including:

  - The configuration policy was displayed as “Unknown” in the client item lists
  - XML events such as Basic Inventory were not accepted by the Privilege Manager server

  This has been resolved by the Mac agent performing additional validation of the agent configuration policy; invalid values will be ignored or replaced by a default value.
- Resolved an issue where commands that use a root shell automatically (**ps**, **su**, `top`, etc) were not successfully blocked when using a **Deny Execute** action without prefacing the command with `sudo`. Now, If a **Deny Execute** action is placed on running `/usr/bin/su`, for example, each of the command lines `su` and `sudo su` are blocked from running in the terminal.
- Resolved an issue that could prevent registration of Macs bound to AD domains that were configured with non-default search paths.
- A fix was implemented to ensure running `sudo` as a command running a bare `sudo` command correctly displays the sudo usage information, instead of running an elevated shell.
- The following fix is available for macOS Monterey and Ventura to address an issue with the Printer Queue not opening:

  - Update the agent to 11.4.3
  - Remove the printer from the Printers & Scanners preference pane
  - Add the printer back into the Printers & Scanners preference pane

  The Printer Queue then opens normally.

11.4.2 Release Notes

Release Schedule

Privilege Manager Cloud Release – Saturday, September 23, 2023

Privilege Manager On-Premise Release - Friday, October 6, 2023

Windows Agent Software

11.4.2168 Bundled Privilege Manager Agent Installer
11.4.2168 Core Thycotic Agent (x64)
11.4.2168 Core Thycotic Agent (x86)
11.4.2168 Application Control Agent (x64)
11.4.2168 Application Control Agent (x86)
11.4.2168 Local Security Solution Agent (x64)
11.4.2168 Local Security Solution Agent (x86)

11.4.2168 Bundled Privilege Manager Core and Directory Services Agent
11.4.2029 Directory Services Agent (x64)

macOS Agent
11.4.2.021 Privilege Manager macOS Agent (Catallina and later)
10.8.27 Privilege Manager macOS Agent (Catalina and previous)

Privilege Manager On-Premise Release - Friday, October 6, 2023

Windows Agent Software
11.4.2169 Application Control Agent (x64)
11.4.2169 Application Control Agent (x86)

When upgrading Privilege Manager to a newer version, Delinea recommends upgrading the Directory Services agent such that both are running on the same release version.
Privilege Managerexclusively supports operating systems (OS) that have not reached their official End of Support. For optimal performance and compatibility, it is recommended to utilize Privilege Manager on a supported and actively maintained OS.
Delinearecommends as a best practice to create system restore points prior to doing system changes such as patches.

Upgrading with Virtual Service Accounts

In version 11.4.2, the **Thycotic Application Control** service is run using a virtual service account named **NT SERVICE\ArelliaACSvc** instead of **NT AUTHORITY\SYSTEM** (LocalSystem). Note that virtual service accounts really are "virtual" in that there isn't a user account being provisioned on the computer. These accounts have been a supported feature since the release of Windows 7 SP1.

By default, all virtual service accounts are members of the group **NT SERVICE\ALL SERVICES**, and Microsoft grants the **Log on as a service** log on right to that group when Windows is installed. If that log on right is revoked from that group the service will not start.

Important: Before upgrading to version 11.4.2 or newer from version 11.4.1 & older, review this information completely and ensure that your runtime environment complies with the stated requirements. Failing to do so will result in the application control service failing to function properly.

Refer to "Virtual Service Accounts" on page 90 in Upgrades.

Certificate Validation for SSPM Agents

For both the Windows Agent and macOS Agent, by default, validate server certificate is turned off. However, if your server domain includes one of these, then validate server certificate will automatically be turned on and the server certificate will be validated:

- .privilegemanagercloud.com
- .privilegemanagercloud.eu
- .privilegemanagercloud.com.au

- .privilegemanagercloud.com.sg
- .privilegemanagercloud.ca

To force this setting to be enabled for use with an on-premise Privilege Manager server via MDM deployment of the agent, refer to the documentation:

Installing Windows Agents
Installing macOS Agents

Privilege Manager Windows Agent Security Update

A local privilege escalation vulnerability that could be exploited to allow access and/or modification of highly privileged system-level folders and files was identified. This impacts all versions of Privilege Manager Agent on Microsoft Windows before v 11.4.1030. This issue is rated High with an 7.8 Common Vulnerability Scoring System (CVSS) score. Please see the CVSS Calculator for details.

This issue has been resolved where Authenticated Justification Message Actions were not properly handling groups marked as Use for deny only, which could result in the action incorrectly producing a success result when a failure result should have been produced.

Fixed in the following versions:
Application Control agent (x32) - 11.4.2169
Application Control Agent (x64) - 11.4.2169

Enhancements

- New policies that support Just In Time (JIT) elevated access have been added to the default Windows Computer Group. JIT elevated access grants temporary administrator access to workstations without having to create unique policies for applications with this need. Any application that requires elevation can be run as Administrator by the user.
- Performance improvements were made to the File Agent Discoverer for the Image Processing Performance report.
- Privilege Manager 11.4.2 allows policies in one Secured Computer Group, along with its permissions, to be moved to another Secured Computer Group. Any role, including custom roles with write permissions assigned to the Secured Computer Group, can edit the policy moved into that Secured Computer Group.

  Note: This update does not extend to the Filters and Actions that were created specifically under the original Secured Group.

- The User Management and Group Management screens now load faster by showing the list of managed and built-in users and groups only. Inventoried users and groups no longer appear by default unless there are less than 200 workstations in that computer group. You can still manage any group or user on those workstations using **Create User** or **Create Group** in the top right of those tables.
- Added a new **Remove** feature to the **Optional** field within the create and modify tasks screens.
- Privilege Manager now allows greater flexibility in elevating or blocking the execution of sudo and commands run under sudo. See "Configuring Block sudo commands for non-admin group users" on page 390.

- On macOS, installer packages (.pkg files) can now be inventoried by uploading them to the Privilege Manager Server (or via the macOS agent file inventory process). Once inventoried, their signing certificates will be available to use in the Digital Certificate filter. This allows Privilege Manager policies to control the installation of .pkg files signed by a particular vendor.
- Policies that include common scenarios for macOS are available in the Workstation Policy Framework. They include the following elevation and monitoring policies.
  - Elevate Common Preference Panes
  - Elevate Xcode
  - Elevate Console
  - Elevate Pakcage Installers
  - Elevate jamf Commands
  - Monitor sudo Usage
  - Monitor Admin Applications

Bug Fixes

- Fixed an issue for the **Application Control - Secondary Hash Exclusions** Config Feed, to ensure it can be installed without errors.
- The Privilege Manager UI can identify managed users which have a mixture of upper and lower case characters within its name.
- The **Prevent File Operations** option in the Restrict File dialog action now functions the same as Disable Context menu options, blocking the context menu entirely. This applies to the agent versions 11.4.2 and above.
- Fixed an issue that was causing all client items to be rebuilt unnecessarily, causing additional network traffic between servers and agents.
- When creating a new **Send Change History Events to Syslog** task you no longer get a default schedule. Now, all templates consistently create a schedule.
- The **User Cannot Change Password** option for the Administrator account under Windows User Management is no longer available due to an unsupported option for the Administrator account on the Windows workstations.

  Note: If the option has been enabled prior to 11.4.2 the upgrade process will automatically set the field to false before disabling in the Privilege Manager Console.

  All other users remain unaffected.
- Fixed issues where the Agents Missing a Policy report was inconsistent with the Policy page Deployment summary.
- Fixed an issue regarding user-configured agent settings, where upgrades could not update defaults, and the **Memory Protection** setting showed incorrectly in the UI.
- Fixed an issue with fully-trusted UWP applications in version 11.4.1. The **User Access Control Consent Prompt Detected** filter now matches a UWP process that was launched via right-click -> **Run as administrator**, as well as a UWP app that is manifested to always run as administrator.

- Fixed an issue where incorrectly edited XML was causing the Application Control policy to fail and show no groups.
- Updated Privilege Manager Console to display the complete resource name. Previously long resource names would appear cut off.
- Fixed an issue that produced errors when importing Azure AD Device data, even when the Device ID changed.
- An issue was fixed that now allows Basic and Hybrid UWP applications to have Justify and Approval actions applied to them by Application Control policies.

  Up through Privilege Manager Agent Version 11.4.1, the UI for the Justify/Approval action did not appear on the user's desktop, errors were logged in the Agent's Event Log, and the UWP application itself would self-terminate when the action failed.

Agent Specific

Windows

- Fixed an issue with the Windows Application Control agent where a long command line could cause the service to stop responding.
- Updated the Windows agent to ensure agents no longer rely on locally cached hashed value of a targeted application when the targeted application has changed.
- Updated the Windows agent to ensure agents no longer rely on locally cached file versions of a targeted application when policy matching. This ensures that audited events correctly show the version number of the application.
- When the LSASS system service process is configured to run as PPL (Protected Process Light), it prevented the resulting Thycotic Application Control service running the ArelliaACSvc.exe program to run properly. Now, the privileges required for the service to start and run properly are explicitly granted to that virtual service account when the native NT service is installed.
  Additionally, the service configuration is modified to prevent the service from starting if the required LSA privileges have been revoked from the virtual service account.
  The following LSA privileges are granted to the virtual service account and must not be revoked or the service will not start or run properly.
  - SeBackupPrivilege
  - SeChangeNotifyPrivilege
  - SeCreateGlobalPrivilege
  - SeCreatePermanentPrivilege
  - SeCreateSymbolicLinkPrivilege
  - SeCreateTokenPrivilege
  - SeDebugPrivilege
  - SeDelegateSessionUserImpersonatePrivilege
  - SeImpersonatePrivilege
  - SeIncreaseBasePriorityPrivilege

- SeIncreaseQuotaPrivilege
- SeIncreaseWorkingSetPrivilege
- SeLoadDriverPrivilege
- SeManageVolumePrivilege
- SeProfileSingleProcessPrivilege
- SeRestorePrivilege
- SeSecurityPrivilege
- SeSystemProfilePrivilege
- SeTakeOwnershipPrivilege
- SeTcbPrivilege

Important: It is necessary to ensure that GPOs (Group Policy Objects), any other Microsoft-supplied system configuration management tools or any third-party products do not revoke or change these LSA privilege assignments.

macOS

- Addressed a performance issue observed in the 11.4.1 release running on macOS Monterey.
- Updating Managed groups from the Privilege Manager server for macOS agents now correctly update the group on the agent if one of the users included does not exist on the agent.

Known Issues

- *Issue*: In certain situations, after logging on to the computer after it has been restarted, it is possible that the very first application elevation request is not properly intercepted and results in the default UAC consent prompt being displayed.

  Resolution: Canceling the consent prompt and immediately retrying the elevation request results in the prompt being intercepted and an application elevation policy being properly applied.
- *Issue*: On older macOS releases, when approval is received for an installer package (.pkg file), but that package is installed by opening it directly rather than from the notification, then the same package is opened a second time and approval is granted, the package may not be elevated as expected when it is re-installed.
  Affected Systems:
  - BigSur 11.7.6 and older
  - Monterey 12.6.5 and older
  - Ventura 13.2.1 and older

  Resolution: Repeat the approval process for the package one more time.
- *Issue*: Sometimes, after installing the Privilege Manager agent on the latest releases of macOS Big Sur and Monterey, the OS fails to prompt the user to approve notifications from Privilege Manager, and the Privilege Manager application does not appear in the Notifications pane of System Preferences.

  Affected System:

- BigSur 11.7.7 and older
- Monterey 12.6.6 and older

Workaround: Restart the Mac. After restarting and logging in, you will be presented with the prompt to approve notifications from Privilege Manager

11.4.1 Release Notes

Release Schedule

- Privilege Manager Cloud Release - Saturday, June 17th, 2023
- Privilege Manager On-Premise Release - Friday July 7th, 2023

When upgrading Privilege Manager to a newer version, Delinea recommends upgrading the Directory Services agent such that both are running on the same release version.

Privilege Managerexclusively supports operating systems (OS) that have not reached their official End of Support. For optimal performance and compatibility, it is recommended to utilize Privilege Manager on a supported and actively maintained OS.

Delinearecommends as a best practice to create system restore points prior to doing system changes such as patches.

Certificate Validation for SSPM Agents

For both the Windows Agent and macOS Agent, by default, validate server certificate is turned off. However, if your server domain includes one of these, then validate server certificate will automatically be turned on and the server certificate will be validated:

.privilegemanagercloud.com .privilegemanagercloud.eu .privilegemanagercloud.com.au .privilegemanagercloud.com.sg .privilegemanagercloud.ca

To force this setting to be enabled for use with an on-premise Privilege Manager server via MDM deployment of the agent, refer to the documentation:

Installing Windows AgentsInstalling macOS Agents

Jamf Applications

The **Synchronize Jamf Applications by Computers** and **Synchronize Jamf Applications by Computer Groups** tasks are no longer supported. Refer to "Example: Synchronize Jamf Computer Groups" on page 641 for updated instructions.

Enhancements

- The Privilege Manager application has been enhanced to support accessibility features that include keyboard navigation in the left navigation panel and top menu bar, keyboard shortcuts, and screen readers that support

tool tips and on-screen controls.

- The Delinea Policy Framework introduces predefined policies as a baseline for policy implementation, along with an intuitive interface that guides the user through policy definition and customization. Predefined policy templates include: Visual Studio Installers, Software Development Tools, Malware Attack Protection, Capture Application Elevation Attempts, and Allow Microsoft Signed Security Catalog.
- The UI now shows additional associations between objects (users, computers, etc.) that were previously hidden.
- Examined reports and removed report parameters that did not actually affect the data presented in the report.
- Added triggers to better detect when a user account is changed, and the managed user settings need to be reapplied.
- Added new trace log messages to help troubleshoot regex command line filters.
- If a scheduled task is still running the next time the schedule comes due, a new instance will not be launched, and an alert will be raised.
- Because using images with duplicate machine SIDs is becoming more common, the option to merge these as duplicates has been removed.
- SysLog tasks that send application action and justification events now have the option to send events from the last x number of days.
- The Computers Without Agent Installations report has been replaced to clearly show computer resources that do not have a Privilege Manager agent installed. This is not an exhaustive list of all computers that may be in an environment. It lists computers synced to Privilege Manager that don't have a corresponding agent registration. This can occur through Active Directory, Azure Active Directory, and other foreign system computer syncs.
- A new report called Computers Without Agent Components has been added that can be used to find computers that have older agents installed or are missing certain Privilege Manager agent components. These machines have at least some parts of the Privilege Manager agent installed.
- SysLog tasks that send application action and justification events now have the option to send events from the last x number of days.
- **Block Local User Management** and **Block Local Group Management** actions are now available to prevent specific sets of Win32 API functions from being called.

Bug Fixes

- Fixed an issue where no error was displayed when deleting a resource has failed.
- Fixed an issue where incorrect user accounts were being displayed in the Group Management view.
- Fixed an issue that caused multiple updates to the same policy items unnecessarily.
- Task Schedule pages now show their own Task History tab with runs associated only with the schedule.
- Fixed an issue that could cause failures to save AD sync settings.
- When using the HTML Approval action, when an approval is submitted and the application re-opened, it will display the existing approval request. Also, if an application is approved for a set amount of time, opening the application will no longer display the approved modal before opening the application.

- Resolved an issue where Admin users attempting to elevate executables through the Windows settings menus caused errors to be seen in the XAML action modals and agent logs.
- Fixed an issue where approval/justification messages failed to display with some UWP apps.
- Fixed an issue where some programs were not being shown in the Remove Programs utility.

Agent Specific

Windows

- Added protections against resetting the password for managed users on the Windows agent, whose password is also being rotated.
- An issue involving Privilege Manager failing to handle 32-bit Win32 desktop applications requiring administrative rights launched by the modern/immersive System Settings UWP application on Windows 10/11 caused the application not to launch properly. This issue is resolved. Multiple error codes are now tested for and an appropriate retry is performed that works equally well for both 32-bit & 64-bit applications.

macOS

- Performing a Disable or Enable of a Managed macOS User will now work as expected on the macOS Agent.
- When macOS Managed Users or Groups are updated from the Privilege Manager Server, the agent will now execute the updated policy upon receiving it.

  Previously the agent would only execute on the defined schedule.
- Resolved an issue where Copy to Applications and similar policies would not always activate when the user's preferred language was set to something other than English.
- If the macOS agent is unable to update the local account password when executing a password rotation policy, it will no longer send the new password to the Privilege Manager Server.
- Resolved an issue where users were not being added/removed to the macOS admin group when the policy was deployed to the macOS agents.
- Fixed an issue where after an extended period of time, the macOS agent's event processor might stop responding to commands.
- Apple included a security update in macOS Ventura 13.3 with an undocumented side effect that disabled Privilege Manager’s ability to apply policies to Installer packages (.pkg files). Apple subsequently included the same change in BigSur 11.7.7 and Monterey 12.6.6, with the same side effect. This release restores the functionality that was disabled by the security update.
- Resolved an issue in which choosing the **Launch** option in the Approval Notification for Installer packages (.pkg files) would not cause the package to be opened and installed.

Known Issues

- *Issue*: On older macOS releases, when approval is received for an installer package (.pkg file), but that package is installed by opening it directly rather than from the notification, then the same package is opened a second time and approval is granted, the package may not be elevated as expected when it is (re-)installed.
  Affected Systems:

- Catalina 10.15.7 and older
- BigSur 11.7.6 and older
- Monterey 12.6.5 and older
- Ventura 13.2.1 and older

Resolution: Repeat the approval process for the package one more time.

- *Issue*: Sometimes, after installing the Privilege Manager agent on the latest releases of macOS Big Sur (11.7.7) and Monterey (12.6.6), the OS fails to prompt the user to approve notifications from Privilege Manager, and the Privilege Manager application does not appear in the Notifications pane of System Preferences.
  Workaround: Restart the Mac. After restarting and logging in, you will be presented with the prompt to approve notifications from Privilege Manager
- User Access Control Consent Dialog Detected filter is not able to detect when a fully-trusted UWP application is launched with **Run as administrator** from a right-click menu.

11.4.0 Release Notes

Release Schedule

- Privilege Manager Cloud Release - Saturday, February 18th, 2023
- Privilege Manager On-Premise Release - Tuesday, March 7th, 2023
- Windows Agent 11.4.1030 - Tuesday, March 14, 2023

Note: When upgrading Privilege Manager to a newer version, Delinea recommends upgrading the Directory Services agent such that both are running on the same release version.

Disclaimer

This issue is not a Delinea issue and the information provided here is being provided as a courtesy.

Problem

After applying the February 14, 2023 Microsoft update KB5022842 (OS Build 20348.1547) on a Virtualized Windows Server 2022 with Secure Boot Enabled and rebooting the server a second time, the machine might crash and not start up. This issue is reproducible without any Delinea products installed on the Windows Server 2022 system.

Cause

Microsoft and VMWare are currently looking into the root cause of the system crash.

The issue arises on the second reboot after installing Microsoft update KB5022842 on Windows Server 2022 running on VMWare vSphere ESXi 6.7 U2/U3 or vSphere ESXi 7.0.x.

Resolution

Refer to the following VMWare article for further information and for steps on how to mitigate/resolve the issue:

Virtual Machine with Windows Server 2022 KB5022842 (OS Build 20348.1547) configured with secure boot enabled not booting up (90947) (vmware.com).

Note: Delinearecommends as a best practice to create system restore points prior to doing system changes such as patches.

Privilege Manager Windows Agent Security Update

A local privilege escalation vulnerability that could be exploited to allow access and/or modification of highly privileged system-level folders and files. This impacts all versions of Privilege Manager Agent on Microsoft Windows before v 11.4.1030. This issue is rated High with an 7.8 Common Vulnerability Scoring System (CVSS) score. Please see the CVSS Calculator for details.

Acknowledgement: Delinea would like to acknowledge Danish Cyber Defence, and Johannes Hatting - IT-Security Specialist, for their role in identifying this vulnerability, and working with our team in its expedited resolution.

Enhancements

- A new setting, **Include Built-In Administrator Account**, allows the built-in administrator account to control services when using a **Restrict Account Permissions on Agent Services (Windows)** policy.
- The Privilege Manager Login screen now returns a generic error containing a unique correlation ID when the login attempt has failed. You can search the correlation ID in the Privilege Manager server logs for additional information and reason for the failure.
- Agent Registration performance improvements were made to the database.
- Windows 11 and Windows Server 2022 have been added to Agent Summary reports.
- Additional IPs have been added to the list of supported IPs for Privilege Manager Cloud. See Privilege Manager Multi-Tenant Cloud Architecture.
- Added the ability to elevate/restrict fully-trusted UWP (Windows Store) Apps like Windows Terminal (Windows 10+) and Notepad (Windows 11+).
- In order to prevent unauthorized systems from sending data to a syslog/SEIM system, users can now use client certificate authentication.

Bug Fixes

- Unacknowledged events are no longer cleared from the Notification page when a **Purge Old Computers** task is run.
- You no longer need to resave User Context filters after importing changes to the membership of a related Azure AD group.
- Fixed an issue that prevented the Privilege Manager agent from provisioning users and groups that had the same name as a user or group in the domain they were attached to.
- The Server no longer sends expired Arellia Certificates to the endpoints.
- Several instances where multiple rows were returned for the same user or group have been fixed.
- The **Import Directory OU** task has been updated with required parameters and no longer produces an error.

- Users logged into Privilege Manager Server with Azure AD login credentials are now redirected to the correct page to re-authenticate after logging out or a session timeout.
- Duplicating file hash filters (Windows and MacOS) that specify a list of hash algorithms works properly now.
- Selecting an Azure AD group for user context filters no longer results in warnings in the agent logs.
- Previously, launching an uninstaller from the Apps and Features, using an elevation policy, would not work because of the restricted token of that Settings app. We've fixed our elevation to handle this case.
- Tasks are cleared from Task Scheduler when the Delinea Agent is uninstalled.
- Referencing Jamf Computer Groups now works the same as other foreign collections.
- Computer names will now be displayed in full across the Privilege Manager Server console. Previously, this was restricted to 16 characters.
- Environments with a large amount of services are supported when selecting services for a scheduled job.
- Unique names are now required for roles. When creating a role, the **Role account name** is used to generate the default **Display Name** and **Account Name**. Additional fields have been added to the Role details page, where you can now modify the **Display Name** and **Description**, along with the pre-existing **Membership** option.
- Selecting all approval requests on the Manage Approvals page now selects just the visible displayed requests.
- The Policy Events report no longer displays an error when a Date\Time filter is defined and a browser refresh is initiated.
- Fixed an issue where some applications with specific version data would cause an invalid XML character error.
- ThycoticOne users can be deleted from Privilege Manager. Existing ThycoticOne users will need to be manually edited to remove the NoDelete attribute via the XML editor.
- Fixed an issue where some sample policies were not being updated to the latest configuration.
- Fixed an issue in previous versions that caused the Service Bus web application to shut down due to inactivity, resulting in the mobile app to no longer functions.
- Fixed an issue where the mobile app could not be used with a user unless that user was directly assigned to a role (indirect through a group would not work).

Agent Specific

Windows

- An issue that caused the agent to be unable to register the **Request Run As Administrator** context menu extension for the .ps1 file type for Windows 11 is fixed. Registry keys and values are now used to perform the context menu extension registration on Windows 11 systems when creating system file associations.
- The 11.4.0 Windows Agent fixes a memory leak caused by the **Parent Process** filter.
- Built-in user accounts can now have an initial random password generated when they are managed, using the new Windows agent. Previously, the password generation process on the agent workstation would error if a user attempted to manage a built-in user and set an initial random password.
- Windows Scheduled Jobs configured with a **Local Security Delete Command** now correctly processes the users and groups.
- Updated the Windows Agent to support files with a path name longer than MAX_PATH characters.

- Fixed consistency issues with updated XAML messages for Windows Actions. When editing custom XAML messages, text is correctly saved.
- For HTML message actions that contain multiple messaging sections, the HTML editor is no longer enabled, in order to preserve the HTML structure. You will still be able to edit the content of the HTML messages through the Item XML editor, if needed.
- Fixed an undersize buffer problem, error handling problem, and data scrubbing problem that caused the ArelliaACSvc.exe process to terminate due to an unhandled exception.

macOS

- Policies that allow command line binaries to run elevated via the sudo command should contain a **Run as Root** action. This allows them to be distinguished from policies to monitor the execution of command-line binaries. A **Run As Root** action is required, even if that action does not perform any action in the policy.

  Note: With this release, this requirement is strictly enforced. Review any such existing policies and add a Run as Root action if needed.

- The **Elevate Privilege Manager Agent Preference Pane (Sample)** and associated **System Preference** filter have been updated to support the opening of the Privilege Manager Preference pane on Catalina and later versions of MacOS, this also includes Ventura.

  The **System Preference** filter has been renamed to **Privilege Manager Preference Pane (MacOs)** the description and file name definitions have also been updated.

  If the sample policy is enabled, post upgrade the Agents will need to refresh their policies before the extended functionality will enabled.

- Managed user/groups or password rotation policies for macOS endpoints with a weekly update schedule that included “Tuesday" would display as “Unknown" on the endpoint and would not be executed as intended. This has been fixed.
- Creating a duplicate **Application Approval Request** (with ServiceNow Request Item Number) Message Action no longer displays incorrectly on the MacOS Agent.
- The Energy Saver, Battery, Lock Screen, Date & Time, and Network Preference Panes in macOS Ventura are now supported. Lock Screen is new in macOS Ventura. Refer to System Preferences documentation for more information.

11.3.3 Release Notes

Note: >When upgrading Privilege Managerto a newer version, Delinea recommends upgrading the Directory Services agent such that both are running on the same release version.

Enhancements

- Added various tooltips to fields within the product.
- The MessageHistory table was unused and has been removed.
- The Policy Events page now defaults to last 3 days to load more quickly, and is restricted to a maximum of 250,000 events.

- Refresh button is now tab-aware in select locations. Refreshing on the membership page of a Secured Computer Group will recalculate the groups membership.
- New maintenance task for purging Group Membership History table.
- Changed default recursive group membership lookup to avoid issues with large nested groups when logging in to Privilege Manager.
- Added an option for Secured Groups to enable selecting an OU and all children to address issues with migrating computers into directed policy groups.

Bug Fixes

- Fixed issue with SAML Authentication Provider where certificates could not be uploaded.
- Fixed structuredClone UI error in some browsers.
- Fixed changing and saving Security tab settings for Secure Computer Groups.
- Fixed sizing of graphs on high resolution monitors.
- Fixed endless spinner on Alerts page when there are no alerts.
- Fixed issue with gracefully handling null responses for report calls.
- Fixed incorrect handling of local users that have the same name as the domain to which the computer belongs.
- Fixed an issue related to AD import that caused database upgrade failures.
- Fixed the Users as Local Administrators report and drilldown to no longer time out on large systems.
- Fixed grid rows to show all text when the row is selected. Grid supports resizable columns.
- Fixed the Computer Group Membership report was updated to prompt for required parameters instead of just displaying no results.
- Fixed issue with license start dates being incorrect for multi-year keys.
- Fixed local account lookup if the account name was the same as the domain to which the computer is connected.
- Fixed issue with policy deployment statistics including computers that did not have the latest version of the policy.
- Fixed issue with upgrades denying pending approvals.
- Fixed issue with inaccurate data on Application Actions drilldown report.
- Fixed issue with Agent Registration State drilldown to properly show last registered date.
- Fixed issue with assigned a computer not being removed from assigned computer groups upon deletion of the computer.
- Fixed report parameter issue that was blocking the Application Metering Events report from displaying data.
- Fixed an issue that caused API calls to produce a 500 error following system maintenance.
- Fixed and issue where the Secret name from Secret Server was not being updated.
- Fixed issue where authentication through a SAML provider would produce 2 audit logon events.

- Fixed an issue with the Thycotic Digital Certificate filter missing the certificate association in some environments.
- Fixed an issue where collection filters were not properly displaying values.

Agent Specific

Windows

- Fixed issue with user context filters not applying to child processes of elevated applications.
- Fixed issue with advanced messages not opening up URLs in the default browser.
- Fixed issue with advanced message crashing.
- Fixed issue with remove programs helper not uninstalling some applications.
- Fixed issue with 32-bit Application Control Agent crashing.
- Changed certain repeating log messages to a trace level.

macOS

- Native macOS agent now supports both Intel and Apple silicon-based hardware.

Known Issues

- An improperly configured policy that uses the Group Member Authenticated Message Action [GMAMA] will result in the policy being erroneously applied to child processes created by a process that already had the policy applied to it. This results in multiple authentication prompts being presented to the user.
- For the 11.3.3.1 macOS Agent support has been introduced for macOS Ventura (13.x) although the following known issues are noted below:
- The Privilege Manager Agent does not currently support policy filtering for System Settings (preference panes) in Ventura.
  - Any policies deployed will not be supported on Ventura at present.
- If the Agent is uninstalled and re-installed Full Disk Access will be required to be granted again in the System Preferences.
  - This is a known issue with version 13.0.x of macOS Ventura. Apple has documented the issue with details here: https://developer.apple.com/documentation/macos-release-notes/macos-13-release-notes/#Endpoint-Security.

11.3.2 Release Notes

Note: When upgrading Privilege Managerto a newer version, Delinea recommends upgrading the Directory Services agent such that both are running on the same release version.

Enhancements

- A new option, **Verify group membership via Domain Controller(s)** allows the user to control how te domain controller is contacted to re-authenticate the user. See the New Group Member Authenticated Message Action in the documentation.
- A new method for adding computer names to a computer group is available using the API. A resource filter is defined by a **Computer by Name Filter** and computer names are populated using a Powershell script. See Creating a Computer Name Filter Collection Query.
- Windows 10 Enterprise for Virtual Desktops (EVD) machines will now consume a Client license within Privilege Manager Server rather than a Server license.

Bug Fixes

- Correct error messages are now returned when incorrect login credentials are entered.
- Resolved an error being displayed when when using XAML notification actions when User Access Control Consent Dialog Detected filter is added as an inclusion filter.
- Issues with the authentication token expiring and not refreshing for large Azure Active Directory imports has been addressed. Azure Active Directory domains with large databases are now correctly synced to the Privilege Manager Server.
- An issue was resolved that caused Local Security data to unnecessarily block the deletion of some users in Privilege Manager.
- When editing a copy of the Restrict File Dialog actions, the Disable Context Menu Options setting was not properly saved. This has been resolved.
- When deleting Active Directory organizational units (OUs) from the UI, some related objects were not properly cleaned up, leading to errors blocking further deletes. Related objects are now properly deleted.
- Privilege Manager has two different versions of the ServiceNow connector, one of them was sending InitiatorUserName and one was not. Now both versions should properly send `InitiatorUserName` with the format `domain\username`.
- Privilege Manager now functions with FIPS enabled in the Windows policy (both agent and server). Upgrade will change the default inventory hash algorithm setting to SHA256 and Authenticode 2. This fixes an error with NTLM authentication when FIPS is enabled on the PM server.

Agent Specific

Windows

- Fixed a problem where elevation fails for **Advanced system settings** when it is launched from **System Settings** and the associated policy contains an approval/justification action.

macOS

- macOS application policies are no longer flagged as invalid when using a message action with the option **Applies To All Processes** when the action **Allow Package Installation** is also used.

11.3.1 Release Notes

Note: When upgrading Privilege Managerto a newer version, Delinea recommends upgrading the Directory Services agent such that both are running on the same release version.

Enhancements

- Workstation User accounts can now be created with a static password or a random password. Refer to User Management.
- For improved usability, the **Details** and **Password** tabs have been combined on the User Management page.
- Azure Active Directory domains now support the Azure Government Cloud instance with a new **Government Instance** setting.

Bug Fixes

- A Policy Priority from the Application Policies page now enforces maximum values of 10,000.
- From the Event Summary widget on the Dashboard,the numbers displayed for categories correctly reflect the amount of events on the Event Summary page.
- Documentation has been updated to clarify the relationship of Product Licenses reports to the actual license values reflect on the Home screen.
- Scheduled Job names have been restricted to prevent scheduling and display issues. Only the following special characters are permitted: ".", "-", "_". and "()".
- If an agent requested a hash filter before collections were updated, the filter would not be properly applied to a policy. We now properly detect collection changes and rebuild these cached items.
- User-defined endpoint groups that previously appeared under the root of a user-defined target now appear in Windows-specific and macOS-specific folders.
- When saving managed User Group updates, a cached definition of the computer Group was saved, potentially reverting recent changes to the computer group. Now, the updated Computer Group is saved with the updates.
- Resolved an issue with multiple policies not triggering in the correct order for the same event. Now, the higher priority policy will always trigger the event first.
- Resolved an issue that caused an error when uploading an MSI file with a SHA256 signature.
- Users can now select secure Computer Groups on the Policy Details page for Computer Groups targeted.
- Previously, a valid signature had to be valid if any signature was present, regardless of the settings. Now, if the setting to require agent event signature is off, both missing an invalid signatures are ignored.

Agent Specific

Windows

- HTML-based actions now pop up in the foreground. Additionally, icons for the user interface have been added to the task tray.

- Elevation of programs located on remote network shares is now working properly across all known and commonly used server and share configurations.
- The icons correctly display on the Privilege Manager Remove Programs Utility.
- The Agent Utility now reflects any policy updates that have occurred since the utility was started.
- Resolved an issue with the update utility for Dell BIOS updates.

macOS

- Fixed an issue where incorrect permissions prevented some administrators from editing the macOS Agent Configuration.

Known Issues

- Computational errors will occur with running local processes that access any of the content on the drive letter made available via Google Drive for Desktop. For example, file inventory operations will fail to access Google Drive for Desktop.
- Policies intended to elevate, require approval/justification, or block/deny access to the the entire Control Panel or to specific applets within it such as Set Time & Date and Time zone. Advanced System Settings may not work 100% of them the time due to how Microsoft has been evolving the implementation of the Control Panel and the System Settings tools.

11.3.0 Release Notes – Server

Enhancements

When upgrading Privilege Managerto a newer version, Delinea recommends upgrading the Directory Services agent such that both are running on the same release version.

- With this version of Privilege Manager, Delinea introduces the new brand design which includes updated colors and logos. For more information, refer to User Interface Updates.
- On the Reports page, under the Local Security section, added a report for "Group Membership By Computer Group (Resource Target)" which returns the same details as the Group Management page for a Computer Group and can be exported as CSV or PDF.
- On the Reports page, under the Local Security section, added a report for "User Membership By Computer Group (Resource Target)" which returns the same details as the User Management page for a Computer Group and can be exported as CSV or PDF.
- New scheduled jobs have been added:
  - Privilege Managerallows the deletion of local User Names and Group Names via the Scheduling function. For more information, refer to Delete Local Users and Groups.
- The **Item Processing Performance** report displays the **agentevent** category, which enables customers to track agent events passed to the server. These events include Application Control, Core, File Inventory, Local Security, and Directory Services.

Cloud

- Added process randomization for out-of-the-box scheduled events to improve overall processing performance.
- Performance improvement for setting up new cloud instances.
- Added **Reset Auth Provider to Thycotic One** task to generate a new client ID and secret, allowing use of new values rather than those stored in the database.
- Implemented process improvements for cloud provisioning tasks that were timing out due to pending app pool recycles.
- Added reports to Cloud Manager for Privilege ManagerCloud instances.

macOS

- To ensure consistent behavior with the Energy Saver preference pane on Monterey, it is recommended that the latest macOS agent be used in conjunction with the Privilege ManagerServer updates:
  - To support the new Energy Saver preference pane on Monterey, the following filter was added:
    - Energy Saver Preference Pane (macOS) – Monterey and Later
  - In support of the Battery preference pane on laptop hardware introduced in Big Sur, the following filter was added:
    - Battery Preference Pane (macOS) – Big Sur and Later

    The following policy was added as an example of how to target Battery and Energy Saver preference panes:
    - Elevate Energy Saver and Battery Preference Panes

Bug Fixes

- If a Privilege ManagerCloud connectivity issue occurs during a page load, a dialogue box will appear with a retry option.
- Recursive AD Groups can cause queries from various resource groups, such as the Directory Service, to time out.
- Privilege Managerdoes not honor connection string settings for connection pool sizes.
- Timing issues cause failures when decrypting the Azure Service Bus connection strings during Privilege Manager startup.
- Following a Privilege Managerupgrade to 11.2.0 and later, various widgets on the diagnostics and dashboard pages spin indefinitely.
- UI displays multiple languages for a management group as opposed to the language specific to the user's region.
- Mac Admin users can update Windows filters and policies; Windows admin users can update macOS filters and policies. Similarly, admin users can create macOS filters using Windows files; Admin users can create Windows filters using macOS files.
- Unable to delete Secured Computer Groups.
- Deleting Secured Computer Groups is blocked.

- System improperly requests and reads the on-premises SID for Azure AD users/groups.
- Certain group memberships are overwritten, depending on the domain size and the order domain objects are processed.

Known Issues

- Adding a Foreign System for Azure AD Domain import and synchronizing wildcard substitutions for Group Display Names and/or User Names may cause errors.
- Shortcut notations, such as `c:\progra~2`, should not be used when specifying a folder/file path in a filter.

11.3 Agent Release Notes

Enhancements

- The **Item Processing Performance** report displays the **agentevent** category, which enables customers to track agent events passed to the server. These events include Application Control, Core, File Inventory, Local Security, and Directory Services.

macOS

- Added support for the Energy Saver preference pane for Monterey.
- Added support for the Battery preference pane for Big Sur and later.

Bug Fixes

- The Application Control agent is unable to remove expired hashes.
- Windows agents do not enforce policies following post-installation reboot.
- There is memory leak in the Application Control agent.
- Privilege Managercollects certificates in the local store, which diminishes performance.
- The "User Access Control Consent Dialog Detected" action does not always replace the Windows UAC prompt on the first UAC challenge after an endpoint reboot.

Windows

- A vulnerability was discovered in the Windows agent which may result in an elevation of privilege attack. It is highly recommended that customers upgrade their agents to version 11.2.3095 or higher to mitigate the exposure. Security Vulnerability Discovered by : Andrew Kisliakov.

11.2.1 Release Notes

Dec 14th, 2021:

Enhancements

Enhancements available with the 11.2.1 release of Privilege Manager. Enhancements are for both versions, On-premises and Cloud, unless otherwise outlined under a specific On-prem or Cloud subtopic.

Note: When upgrading Privilege Managerto a newer version, Delinea recommends upgrading the Directory Services Agent so that both are running on the same release version.

- The granularity of auto-merge is enhanced to allow administrators to choose when registering agents are merged, based on machine SID, Active Directory account SID, domain\computer name and Azure AD device ID.
- Enhancements across the application better reflect conditions that exist with duplicate resources and domain entries. These enhancements appear as new tasks. Reports that support certain conditions are also added.

  Note: In order to resolve any issues with duplicate IDs, these tasks must be run manually.

  - There are two Server Tasks that are available to run the merge actions if registration has already been completed. Note: These tasks are specifically used for merging duplicate IDs; they can not be used to merge domains.
    - **Merge Duplicate Resources** - This task attempts to merge any duplicate values it finds based on the set options.
    - **Merge Specific Resources** - This task merges one or more resources into a selected target resource, regardless of whether they have any duplicate data.
  - There are three new tasks for domain sync improvements:
    - **Merge Duplicate Active Directory Domains** - This task removes unwanted duplicate entries, along with any children of the duplicate domain that are found with the Duplicate Active Directory Domain Merge Candidates report.
    - **Purge Old Unmanaged AD Computers** - This task removes old unmanaged AD computers, which have been around for the default 90 days. The task allows the user to adjust the query with a user-defined number of days.
    - **Remove Active Directory Domain** - This task is added to the maintenance config feed for customers having trouble deleting a domain.
  - The **Users and Groups with Duplicate SIDs** report is renamed to Resources with Duplicate Global Identities (Domain\Computer name), in order to better match it to the merge actions it reports.
  - New Diagnostic reports are available that support the new auto-merge tasks for duplicate IDs. Note: These reports indicate that there are duplicate resources that should be addressed by the customer, using the **Merge Duplicate Resources** and **Merge Specific Resources** tasks. The reports do NOT indicate duplicate domains. They include:
    - Resources with Duplicate Azure Device IDs, lists Computers associated with the Privilege ManagerServer that have identical Device IDs.
    - Resources with Duplicate machine (Domain) SIDs, lists Computers associated with the Privilege ManagerServer that have identical Domain SIDs.
    - Resources with Duplicate Account SIDs, lists Computers, Domain User, and Domain Groups associated with the Privilege ManagerServer, that have identical Account SIDs.

- **Duplicate Active Directory Domain Merge Candidates** This report identifies any existing Active Directory Domains that have been duplicated. Refer to the new Merge Duplicate Active Directory Domains task to address these duplicates.

- The App Registrations in Azure no longer require the Azure Active Directory permissions and can use the Microsoft Graph. Setting Up Azure Active Directory Integration in Privilege Manager now reflects an update for the change from using Azure Graph API to Microsoft Graph API.

  Note: The Azure AD Graph APIs are scheduled to be deprecated by Microsoft by mid-2022, and replaced with the Microsoft Graph APIs. While support for the Microsoft Graph APIs has been added, any existing configurations that use the older Azure AD Graph APIs will not be affected, and will remain functional. However, it is highly recommended that new installs be configured to use only the Microsoft Graph APIs, so they will not be affected when the Azure AD Graph APIs are deprecated in 2022. If both APIs are currently configured to work in your Privilege Managerinstance, no change should be necessary, as the Microsoft Graph APIs will continue with full functionality when the Azure AD Graph APIs are deprecated.

- Email notifications for approvals now have an updated link for the VirusTotal page.
- A new field, **InitiatorUserName**, is added to the Approval Request data in the ServiceNow integration. This field is always in the format DOMAIN\USERNAME. Conversely, the **UserName** field is intended to be a display name and can change depending on how it was created or updated. The behavior of **UserName** will not change. So, if you require a consistent value, use **InitiatorUserName** instead.
- Screen reader support in Windows Advanced HTML Message actions is improved.
- The client item database performance on the agent is improved.

macOS Specific

- Monterey support is added.
- Universal binaries in the agent inventory are fully inventoried.

Windows Specific

- Windows 11 is supported.

  Note: Privilege Managerdoes not currently support Windows Store Apps.

Bug Fixes

- Merging domains now properly handles resources that already have an association to both source and target domains.
- We now check to see if a reference update will create a duplicate Active Directory domain, and if so, we simply remove it.
- Fixed a bug where File Scan commands would not properly inventory a file targeted by a File Specification filter.
- Computers with only the core and Directory Services agent installed no longer consume a product license.
- Warning messages in the agent log about the database being in the wrong location are fixed.

- Client items are scanned and carefully inspected so that only a small subset of required updates are modified during installs. (In prior versions, all client items were resaved, forcing large updates on agents.)
- Group management policies no longer send a full local user and group inventory after each run. Instead, inventory is only sent if a change in the group membership is detected and inventory has not already been sent in the last hour.
- A space in the secondary file path filter, that prevented the filter from being applied correctly, is no longer an issue.
- Errors are not displayed when saving managed local administrator passwords.
- Error handling is improved when saving passwords for Admins in the User Interface.
- The export of files with long names no longer gets truncated and loses the file extension.
- Computers with only the core Directory Services agent installed no longer consume a product license.
- When setting up and running the Email Scheduled task, emails are now triggered to be sent.
- An error no longer occurs when viewing the Task Scheduler history for a user that includes a single quote (') in the user name.
- Local user passwords are no longer set back to the initial password after they are previously randomized.

macOS Specific

- The Privilege Managersudo plugin no longer outputs the "Evaluating command ..." message on the terminal when the sudo command is run.

Agent Specific

- Unix/Linux agent crashes during registration when FIPs is enabled on the agent.
- Agents now stream messages from/to the server, so if the list of policies and filters for an endpoint is very large, the "MaxReceivedMessageSize" error message is no longer encountered.

Agent Specific

- Unix/Linux agent crashes during registration when FIPs is enabled on the agent.
- Agents now stream messages from/to the server, so if the list of policies and filters for an endpoint is very large, the "MaxReceivedMessageSize" error message is no longer encountered.
- The Application Control agent is unable to remove expired hashes.
- Ensure Windows agents start enforcing policies following post installation reboot.
- Address slowness when users attempt to launch applications.
- Address memory leak in Application Control Agent.
- HTML based approval actions cause an error on the Agent.
- Agent reloads Application Control policies and filters after update check.
- Major performance impact on certain PCs after updating Altiris.

Known Issues

- If an agent requests a hash filter before collections are updated, the following occurs:
  - The hash filter is cached without a hash date.
  - The filter is not properly applied to any policy the filter is associated with.
- When creating an Azure AD in Privilege Manager, use the company DNS name instead of the *.onmicrosoft.com name. If *.onmicrosoft.com is used, a duplicate Azure AD system is created when a local user and group inventory is performed where Azure AD Users are present.

  To fix the issue, follow these steps:

  1. If AAD is used to authenticate to Privilege Manager, ensure that an alternate administrator login is enabled.
  2. Disable AAD as an authentication mechanism.
  3. Delete the duplicate AAD system from Privilege Manager.
  4. Edit the AAD system in Privilege Managerto use the DNS name and save.
  5. Reenable AAD for authentication.
  6. Save and test.
- We do not support elevation for Windows Store applications.
- Upgrades may fail when spanning multiple versions. Refer to Troubleshooting Failing Upgrades.

Deprecations

- The UNC Allow Policy Template configuration feed has been removed from the Config Feeds space.

11.2.0 Release Notes

Sep 14th, 2021:

Enhancements

Enhancements available with the 11.2.0 release of Privilege Manager. Enhancements are for both versions, On-Premises and Cloud, unless otherwise outlined under a specific On-Premise or Cloud subtopic.

- Added support for "Secured Computer Groups" on page 435. With this new feature the former Roles option in the Admin menu was renamed to Security and a Configuration tab was added to support custom scoping of user roles to Target Computer or AD Domain groups.
- New fields were added to the User Context Filter to allow targeting of an account (user or group) by SID, even if that account has not yet been inventoried in the server.
- Added a Role Membership tab to user details page for easy role membership verification and changes, like role removal and add to new role options.
- Added a Windows Registry Inventory client task to create a Windows Registry Inventory report.
- Multiple SAML provider support via **Create** option on the SAML Providers Foreign Systems page. Multiple SAML Providers can be set up and Privilege Manager verifies the uniqueness of the Issuer ID.

- Authentication Provider changes are disabled for the provider the current user is logged in with.
- Azure Active Directory groups are not supported for Advanced Message Actions that require authentication by a member of the group. As such, the **By member of the group** selections only show groups that have an AD SID (not pure Azure AD groups).
- The User Access Control Consent Dialog Detect filter was changed to also catch UAC prompts run for MSI installer file types.

Windows Specific

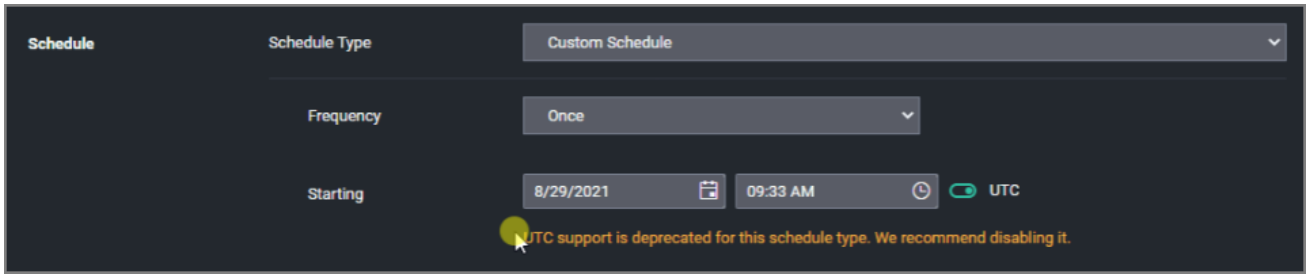
- Added rich text or WYSIWYG Advanced Display Message Action editing support. Deny and Warning prompts, Approvals (online only in v11.2.0), and Justification messages are supported by the new **Display Advanced Message (HTML)** template. Other changes delivered with this feature enhancement:
  - Error message improvements in the log viewer to provide better error details around message actions.
- The Global Application Control policy path exclusions can be configured via the Windows Agent Configuration policy.

macOS Specific

- Introduction of the native event uploader, making the Retry errored TMS Events - Catalina and later (macOS) policy obsolete for Privilege Manager macOS agents v11.2 or later.
- Added support for App Translocation when evaluating the App Bundle Filter Path property. If an App Bundle is run from an App Translocation path, its original path will be evaluated properly against the Filter's Bundle Path property.
- RegEx support when evaluating the Bundle Path property of an App Bundle Filter. This allows an App Bundle Filter to target a path based on RegEx and makes App Bundle Filters more flexible.
- Running the Uninstall.sh script now fully removes all macOS agent artifacts on an endpoint.

Feature Deprecations

- Removed the delete option for Authentication providers if currently active.
- UTC support on Tasks schedules has been deprecated. Delinea recommends that all customized Tasks currently using UTC are changed to have the UTC switch turned off.



macOS Specific

- The **Allow Copy to /Applications/ Directory**action is deprecated and not supported in v11.2 and higher agents. Use the **Copy Install Application Filter** instead, to install to the /Applications folder.

  This deprecation only impacts the v11.2.x macOS agents, older agents will continue to work with **Allow Copy** and drag and drop.
- The Finder Sync Extension used to expose the self-elevate Finder context menu has been removed.

Bug Fixes

- Unacknowledged Events and Tasks in 'Ready' state are not clearing in the console.
- When an Agent registers without knowledge of the AD Domain SID, duplicate AD Domains are created.
- Following an Agent install the Computer/Agent IDs are not merging as expected.
- When importing items the *Overwrite Existing Items* checkbox does not function as expected. Refer to Importing Items for details on the specific import conditions based on checkbox selection.
- Updating WMI Data fails on systems where the UUID remains the same after a change to the operating system, WindowsDirectory, or BootDevice.
- Azure Groups are not being pushed to endpoints.
- 504 timeout error reported on loading of "Group Policies - Administrator Built-In Managed Group".
- Dependencies prevent Purge File Undiscovered and Purge Old Computer maintenance tasks from purging correctly and freeing up licenses.
- Authentication provider changes do not trigger an application pool recycle.
- The User Management Policy for built-in accounts displays the incorrect policy.
- The information under Settings on the Authenticated Justification Message Action is incorrect, the information only pertains to the "By a member of the group" option and not to all settings.
- The UTC Time option does not work with scheduled Email tasks.
- Expired licenses are not deleted from the server.

Cloud Specific

- AD Containers are not recognized by OU Computer Group Filter.
- Cloud instances are showing the "No Valid Support License" banner.
- Setting up and running the Email Scheduled task does not trigger emails to be sent.
- View Password role does not immediately work after system upgrade.

macOS Specific

- File Specification Filter does not support RegEx as intended.
- In versions prior to 11.2 the Uninstall.sh script did not fully remove all artifacts. The following files

- `/var/db/receipts/com.thycotic.agent.bom`
- `/var/db/receipts/com.thycotic.agent.plist`

remained.

Running pkgutil --files com.thycotic.agent should report the following:

```
No receipt for 'com.thycotic.agent' found at '/'.
```

Known Issues

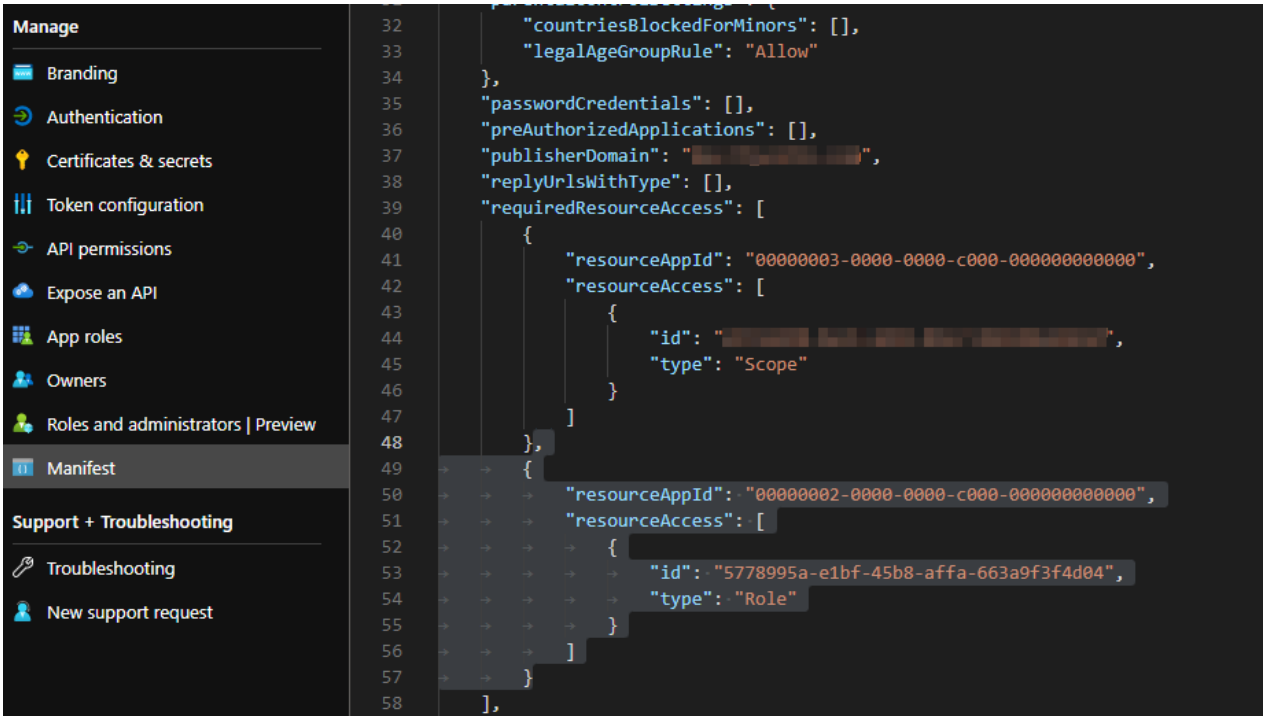
- A change was made when upgrading to the 11.2.0 Release of Privilege Manager that forces a renewed save of all items to ensure they are in their correct states. To an agent, this re-save looks like an update to all of the existing policies and groups and will force a call back to the Privilege Manager Server to ensure it has all the updated policies and correct data. This causes all agents to call back to the server, generating a large amount of traffic while the agents attempt to get the full updated policy set. This impacts network traffic and slows Server processes while the agents are calling back for their updates. The amount of slowdown that the Server process experiences will depend on the number of agents that are attempting to update.

  This can potentially cause a backup if new policies are added or existing policies are being modified and the updates are trying to be sent out, as those updates will be delayed until the update from the re-save is completed.

  For on-premise installations of Privilege Manager version 11.2.0, if you are seeing a large increase in network traffic and Server bandwidth, this is a potential cause. Once all the Agents have been updated with the policies, you should see traffic and resources return to normal.
- Deleting a Parent Targeted Group with a child group will throw an exception message, while partially performing a delete on certain items. As a workaround, first delete the child group before deleting the parent.
- If a block policy is duplicated and used to create another policy to add **Exclusions**, the customized policy will be listed under *Elevate* vs. *Block* policies on the Application Policies page.
- No Domain name is listed under Global Account Details when looking at Azure AD users and groups in the resource explorer.
- Due to the Azure Graph API deprecation in the Azure Portal, manual steps are required to set up the Azure AD Foreign Systems integration:
  1. When you get the Azure Graph API deprecation error while on steps 13 through 15 of this procedure, in the left Manage menu, navigate to **Manifest**.
  2. Copy and paste this text into the json file:

     ```
     ERROR: Invalid Code Highlighting Language
     ```

Refer to the sample image below:



macOS Specific

- App Translocation path resolution does not work on Catalina 10.15.7 (19H1323). This affects App Bundle Filters using the Bundle Path property and File Quarantine Actions. Feedback FB9553808 has been filed for reference.

Clarifications

- Added a topic to demonstrate how to block all sudo commands, while allowing specific exceptions. Refer to "macOS Privilege Manager Sudo Plugin" on page 154.

11.1.1 Hotfix Release Notes

July 3rd, 2021:

Privilege Manager v11.1.1 is a hotfix release to resolve issues discovered in v11.0.0 and v11.1.0 instance and agent deployments.

Bug Fixes

- Parameter Name for Import Azure Users/Groups task is incorrect.
- Indexes missing or duplicated for resource key items.
- Computer Group Based on Azure AD Security Group Not Showing Correct Machines.
- The Group Member Authentication Action is unable to resolve Azure AD groups to allow authentication.

- The Import Specific Azure AD Users and Groups task does not resolve correctly against the specified user or group name.
- The Justify Action message in policies errors out and does not allow a user to run an application as intended by the policy.

Agents

- Improvements for agent database file locations.

Security

- Removal of account name information from GET method for CreateItemByRoleType.

Known Issues

- When a Justification Message action is triggered by an application control policy for an application process that is started via commandline, the agent creates an error. The workaround is, to exclude admins from the justification request and to use a policy with an Advanced Message Action.

11.1.0 Release Notes

June 15th, 2021:

Enhancements

Enhancements available with the 11.1.0 release of Privilege Manager. Enhancements are for both versions, On-premises and Cloud, unless otherwise outlined under a specific On-Premise or Cloud subtopic.

- SAML Support
  - Only one SAML connection/foreign systems configuration is supported.
  - Tested with Okta, Centrify, GSuite and others, documentation examples based on Okta and GSuite integration.
- Improved Azure AD support for:
  - User Context Filters: Azure AD users have 2 SID values. These are mapped and handled on the backend.
  - Group Policies:
    - Add/remove Azure AD users from group policies
    - Add Azure AD user SID to local machine group
- Renamed Group Policies to Group Management.
- Renamed User Policies to User Management.
- Reorganization of the Server tasks as it relates to Foreign Systems and Directory Services tasks. Created new component entry Directory Services Maintenance Tasks.
- In support of **Computer Name Pattern Collections**, the Computer by Name Pattern Query was added to Privilege Manager. The query allows to create custom collections containing a subset of computers based on a wild card supported name query.

- Added a framework that allows real-time status reporting of running server-side tasks. This is currently available for the AD Import task only.
- Privilege Manager now automatically sets the home directory path during provisioning.
- The Security Descriptor Agent Discoverer has been removed for new installations and will be disabled during system upgrades from pre 11.1.0 versions.
- Standardized Privilege Manager logout process to remove access token on logout.
- Console Audit Logs can be sent to a syslog connector, for example to Splunk.
- New View Password role added to Role Management.
- Commandline arguments added to policy feedback and approvals.
- Updated About page. Refer to "Viewing the About Page" on page 8. Added Privilege Manager product version details and 3rd party web licenses information to the page.
- Added Config Feeds for Thycotic Policy Framework quick start policies that improve the initial Privilege Manager configuration experience.

macOS Specific

- Added support for File Inventory of Application Bundles as zip files via File Upload.
- Added support for macOS Homebrew installer.
  - As part of the Homebrew installer support, added a new parameter to the Just-in-Time Group Membership Action to better determine the sudo plugin usage.
- Added Run as User action that is leveraged by the sudo plugin to run arbitrary commands as a specified user.
- Added CLI Approval Message action, which allows administrators to prompt command line users on macOS endpoints for an approval request.
- Added CLI Justification Message action, which prompts the user for a justification when using Terminal to execute commands and scripts under sudo.

Unix/Linux Specific

- User and group inventory for reports.
- Setting to delay password for "X" times after first login.
- Added File Hash filter support.
- Added Run as User action, which allows a command the user runs on an endpoint to be treated as if a different user ran it.
- Added CLI Approval Message action, which allows administrators to prompt command line users on Unix/Linux endpoints for an approval request.
- Added CLI Justification Message action, which can be used to provide a customized multi-line justification question to the user.

Security

- Implemented friendly error messages when registration fails due to invalid BaseURL, excluding stack trace details.
- Added support for additional Hash algorithms (Limitation: newer security hash algorithms are only supported on v11.1 Agents and later.)

  Note: Customers are encouraged to change their policies and filters with SHA1 specification to SHA256 or other supported algorithms.

API

- New API to run an existing report and return the results.
- New API to run a task based on a specified task Id.

Integrations/Foreign Systems

- New ServiceNow integration via available ServiceNow Application in the ServiceNow App Store. The ServiceNow app requires a Privilege Manager Foreign Systems setup that includes webhooks configuration. The Privilege Manager ServiceNow app provides the following functionality:
  - Approval/denial
  - Time based approvals
  - Privilege Manager approval process support
  - Records approvals from outside normal flow

Bugs Fixed

- The Resources page is not showing any computers under Organizational Units.
- Agent registration not automatically merging with Azure AD Devices data.
- Loading groups from Not Well-Known Local Group Summary or Well-Known Group Summary pages creates an error.
- Retrieving large numbers of Users and Groups can be slow.
- The application control agent creates an error when uploading a file to OneNote 2008 notebook.
- When a new managed user is created, the original created password is reset, preventing user login.
- Justification and approval messages are not working when used with networked drive letters in the path properties.
- Computer Groups are not always picking up all added endpoints.
- Password changes for standard users are not honored.
- UAC triggers false positive detection messages.
- Running Privilege Manager: Task Purge Maintenance does not work for Correlated Change History.

- ArelliaDisplayXAMLaction.exe inherits elevation from parent policy when the *Add Administrative Rights* and/or *Unrestricted* actions are included in a blocking policy.
- The Event Summary widget does not reflect changes when changing the associated resource target filter.
- Once the number of events crosses ~21 Million, trimming does not work.
- An issue with the Ams.SimpleWorkerTask table causes tasks not to run while agent events are processed.
- The agent summary by OS report is not reflecting the correct numbers.
- Path exclusion changes are not saved.

Cloud

- UI stops responding while trying to select "Security Group" as an option to add computers to a computer group.
- Azure Only Accounts are required for when Azure AD Authentication is configured.
- The task scheduler does not correctly reflect history for tasks with single quotation marks.
- 504 timeout error reported on loading of "Group Policies - Administrator Built-In Managed Group".

macOS

- macOS justification policy ends the script targeted by a sudo plugin policy.
- The sudo plugin fails to elevate binary with path relative to current directory.
- Users added to multiple groups via macOS Just-in-Time Group Membership Action are only removed from the first but not all groups automatically.
- On agent installation, a Privilege Manager Server URL with a port number is not saved properly.

Known Issues

- If your Privilege Manager instance experiences database performance issues following an upgrade to Privilege Manager v11.x, reach out to Delinea Support for assistance on resolving an indexing issue. This issue has been resolved with the v11.1.1 hotfix release in July 2021.
- Privilege Manager Agents v10.8 and up, might prevent user login when **USB over IP** options are enabled for eCatcher or eBuddy setups. If you encounter an issue, disable the **USB over IP** option.
- The Alerts page does not display file name details under the Name column.
- When Authentication providers are changed, an application pool recycle might be required as indicated via error message.
- When using the latest Privilege Manager agents with old Privilege Manager Server version, like v10.6, policies on the endpoint might not be available. The workaround is to run the Resource and Collection Targeting Update Task on the policy until the endpoint is updated.
- The Setup Add/Upgrades Feature page fails to provide new package information, if the Privilege Manager server is installed on a Windows 2016 system that is also configured as a domain controller.
- The File Hash Filter for Authenticode does not work. This is no longer supported with the new hash algorithms.

macOS

- One-time approvals are not properly recognized when using the latest Privilege Manager agent with older versions of Privilege Manager Server (e.g. v10.5, v10.6, v10.7). In this scenario, once approved, the user will be prompted with another approval request. However, time-based approvals work (within the approved time period). The workaround to one-time approvals is to use a time-based approval.
- On a Safari browser, the option to print licenses via the About page does not render.

Documentation Clarifications

- Allow Listing Policies without Actions

11.0.0 Release Notes

February 24th, 2021:

Enhancements

Enhancements available with the 11.0.0 release of Privilege Manager. Enhancements are for both versions, On-premises and Cloud, unless otherwise outlined under a specific On-prem or Cloud subtopic.

- Renamed **Suppress UAC** Action to **Suppress UAC (Legacy)**. Refer to Default Actions and Adjust Process Rights Action.
- The Remove Program Utility does not require process elevation going forward. With this change a new sample policy was added to Privilege Manager. The **Elevate Privilege Manager Remove Programs Policy Children Policy (Sample)** policy should be activated on endpoints that are configured to use the Remove Program Utility. This policy elevates the uninstallers only after an approval request has been granted.
- Filter validations for application control policies.
  - Conflicting filters in application policies are reported, preventing a policy from being saved or activated.
  - Non-application filters cannot be used as the only filter on an application policy or added as an application target.
- Added Observed Parent Processes reports for discovered events.
- Commandline information support on Server reports for Windows and macOS systems.
- Added computer SID registration information to be available via resource manager computer global account data.
- General user interface improvements, focused field indicators, etc.
  - Overhaul of statistics pages for User Policies.
  - Overhaul of "Configuration Feeds" on page 663.
  - Licensing page updates.
  - Scheduler updates.
  - Reports and Gauges.
- New integration, "Jamf Integration" on page 634, to allow users to:

  - Import Smart and Static Computer Groups and Computers.
  - Import installed applications on Jamf endpoints as discovered resources and create filters.
  - Rollout Privilege Manager Agents on to Jamf Endpoints.
- The Silverlight console has reached its EOL and all support has been removed from Privilege Manager release version 11.

macOS

- Added Apple® silicon support.
- Added Authorization DB handler.
- Rich text editing of end user prompts (message actions) via HTML editor.
- Added commandline parameters for macOS binaries in Manage Approvals for the approval request.

Linux

- New Unix/Linux OS support in the form of an Agent connecting to the Privilege Manager Server to exchange policies and events.
- Role support for Unix/Linux Administrators.
- Added Filters, Actions, and Computer Group support for "Unix/Linux Computers" on page 398.

Agents

- Service method for agents to post events via REST (JSON).

Security

- Added Strict-Transport-Security header to 301/400/403 http responses.
- Improved path traversal and invalid header handling.
- Client-side password complexity check improvements.
- API endpoint authentication improvements.

Bug Fixes

- Folder View loads slowly for large resources with over 200K endpoints.
- No option to specify different .NET framework versions for combined installations of Secret Server and Privilege Manager.
  - Privilege Manager on-premises does not work with Azure Service Bus if the web server is set to use only TLS 1.2.
- Summary of Application Actions by Product Version Reports.
- BSOD error following a Windows system update.
- **Send SysLog ...** template based tasks to send logs to server fails.
- When adding a Persona, not all configuration options are visible in UI.

- The Application Control Service is creating a conflict when saving or printing Excel or Word files.
- Local user logout does not work correctly, preventing another local user from logging in.
- Errors in exported Agent Log file are not displayed.
- User accounts in a child domain do not appear as members of a local group.
- Folder View loads slowly for large resources with over 200K endpoints.
- The Administrator group is showing up twice when viewing the Group Policies section.
- User and group inventory may not reflect proper group membership the first time it runs on the endpoints. Subsequent runs will finish processing that information and will be accurate.
- Users removed from Security Group in AD still show as members of the AD group inside Privilege Manager.

Cloud

- Creating a new managed user through macOS user policies and adding that new user to a newly created user policy on Privilege Manager Cloud an *.outlets* exception error is returned.

macOS

- macOS endpoint restart is blocked on macOS 10.15.7 (19H1030) when a policy targets PKG installation.
- When the agent needs to generate a UUID instead of relying on the Hardware UUID for the AgentId, multiple self-signed certificates are created in the System keychain.
- The KEXT and SYSEX flavors of the macOS agent can experience high memory utilization during File Inventory.
- With the SYSEX flavor of the macOS agent, a policy targeting PKG installation results in multiple authentication prompts to be triggered.
- Packages installed via `/usr/sbin/installer` fail to complete. (Delivered in April 2021 macOS agent hotfix.)
- The elevation of copying an app bundle to Applications or moving it to the trash would sometimes prompt for admin credentials on Big Sur.
- When the sudo plugin is unable to connect to the system extension, the user is unable to execute commands via sudo.
- Newly created users do not show up under the associated group if the user is a managed macOS user.

Known Issues

- Upgrading to Privilege Manager 10.8 or later from version prior to Privilege Manager 10.8.0 causes a task to run to merge computer groups and remove unused system computer groups. This primarily affects the Application Control policies that are using resource targets/computer groups named **All Windows Computers with Application Control Agent Installed**. With 10.8, those policies will use the **Windows Computers** computer group and macOS will use **macOS Computers**.

  If you want to prevent this automatic merge, modify the XML of this item:

  `PrivilegeManager/#/item/xml/b2e02684-d154-48ca-9987-12b1759df822`

Add on line 2 `<adc:Attributes>NoModify</adc:Attributes>`.

- Offline upgrades on **multiple** servers will need to be done manually.
- With the Safari Browser, the behavior for default selection on drop-down menus might vary from other browsers.

macOS Specific

- On endpoints using OneDrive, GoogleDrive, DropBox, or similar extensions, the endpoint will take about 2 min to correctly initialize the Finder Extension functionality after enabling the extension or after the upgrade to 10.8 with an enabled extension.
- If you have a policy allowing management of the /Applications folder via the Copy Install Application filter, deleting multiple applications from the /Applications folder will result in a dialog prompting for administrator credentials. The workaround is to have your end-users delete applications one at a time.
- If you have enabled the Elevate Privilege Manager Agent Preference Pane (Sample) policy to elevate the Agent preference pane and you wish to target Big Sur, you will need to duplicate it and change the File Names to:

  `legacyLoader;legacyLoader-x86_64`
- If you have already duplicated the Elevate Privilege Manager Agent Preference Pane (Sample) policy to elevate the Agent preference pane and you wish to target Big Sur, you will need to change the File Names to:

  `legacyLoader;legacyLoader-x86_64`

Agent Specific

Windows

- The latest Application Control Agent released with Privilege Manager version 11 is not compatible with the driver verifier tool for Windows 10 version 1507. Any endpoints on Windows 10 version 1507 should remain on the 10.8 version of the Application Control Agent until the endpoint can be upgraded to a newer Windows 10 version.

Unix/Linux

- Registering Unix/Linux endpoints to the default target can take up to 15 min.

10.8.2 Release Notes

December 2nd, 2020:

Enhancements

Enhancements available with the 10.8.2 release of Privilege Manager. Enhancements are for both versions, On-premises and Cloud, unless otherwise outlined under a specific On-prem or Cloud subtopic.

- Added CorrelationID support to Server Logs.
- Added Complex Password Policy enforcement for Privilege Manager users.
- Added API Client User logout option via delete method on API Authentication endpoint.
- Added Visual Studio Installer Elevation example policy and filters to configuration feeds.

Security

- Added Process Hollowing prevention for elevated applications. The 10.8.2 Privilege Manager agent adds memory checks for all processes that are elevated via Privilege Manager.
- Return of generic "Invalid username or password" messages.
- Unknown code fallback to generic error message, such as "unable to login".
- Generic HTTP response messages.
- Removed ASP.Net MVC Default HTTP Headers information.
- Updated jQuery to latest version.
- Updated Handlebars to latest version.
- Privilege Manager Cloud server side enforcement of TLS 1.2. On-premises instances can be configured to enforce TLS 1.2 at the OS level.

macOS

- In support of Apple's Catalina and Big Sur macOS System Extension based security enhancements, a "Installing macOS Agents" on page 63 is made available.
- New Just-in-Time (JIT) Group Membership action for elevation/approval policies.
- Added elevation support for move to trash bin when standard user is deleting from /Applications directory.
- Modified policy with Allow Package Installation action workflow behavior for .pkg installs on macOS endpoints.
- The **AdjustEffectiveProcessRightsContract** action has been deprecated for endpoints running macOS Big Sur. The **Run as Root** action has to be used in policies instead.
- Added SUDO Plugin for elevating from command line. Refer to Sudo Plugin. Policies that previously just elevated a process no longer work and the elevation has to be run via sudo instead.
- Added **All macOS Big Sur Computers** Filter, with membership defined as any macOS Big Sur endpoint having an agent installed and registered.
- The default policy **Retry errored TMS Events - Catalina (macOS)** has been renamed to **Retry errored TMS Events - Catalina and later (macOS)**.
- The default policy **Retry errored TMS Events - Catalina and later (macOS)** Computer Groups Targeted property has been changed to **All macOS Catalina and Later Computers with Application Control Agent Installed (Target)**.

Agent Pertaining to Big Sur and Catalina

There are several features available with the KEXT version of the agent which are deprecated in the SYSEX version. There are others that are supported, but may require a change to policy configuration and/or user workflows.

Deprecated

- Allow Self-Elevate via Finder Extension – This feature provided the limited ability to right-click an application and have it run elevated. Depending on the application and how it was implemented, this may have had limited

success for end-users.

- Run as Root applied to application bundles – This feature provided the limited ability to have an application bundle run elevated when it was launched via Finder. Depending on the application and how it was implemented, this may have had limited success for end-users.
- Run as Custom User, Run as Print Admin User – These Adjust Effective Process Rights actions are deprecated.

Supported, but may require workflow changes

- Run as Root applied to command-line binaries – If you have policies that elevate specific command-line binaries (e.g. systemsetup), you will need to inform your end-users that they should now precede these commands with sudo. This takes advantage of the new sudo plugin feature for elevating command-line binaries.* Endpoint Security system extension (SYSEX) replacing most functionality previously provided by the Kernel Extension (KEXT).

Bug Fixes

- The KEXT and SYSEX flavors of the macOS agent can experience high memory utilization during File Inventory.
- The 10.8.1 based Policy Events page does not always load correctly.
- Users removed from a Security Group in AD still show as members of the AD group inside Privilege Manager.
- Logging out does not invalidate the session/cookies that may have been previously stored/cached during a valid logon session.
- Changing the API Client User secret after token issuance, does not force an authorization error and logout.
- Approval reports don't provide drill-down details when accessed.
- X-Powered-By information returned in 301 and 400 http responses.
- Provide detailed DB error messages in log file only.
- Provide detailed error message via log file only.
- The Administrators group is showing up twice when viewing the Group Policies section.
- License counts are not correctly reflected per OS.
- Intermittent failure on approval requests.
- Saving Excel and Word files on SharePoint, MS Query, and Excel print issues due to Application Control Service

Known Issues

- The combined installer released with Secret Server 10.9.000005/32 does not contain a NuGet folder as provided with previous combined installers. Customers can use the download resource link provided via the Software Downloads topic to download the Privilege Manager Application Files for use with their manual and/or offline installs/upgrades. Refer to Manual Installation - Installing as a Virtual Directory for details.
- User and group inventory may not reflect proper group membership the first time it runs on the endpoints. Subsequent runs will finish processing that information and will be accurate.
- With the Safari Browser, the behavior for default selection on drop-down menus might vary from other browsers.

macOS Specific

- On endpoints using OneDrive, GoogleDrive, DropBox, or similar extensions, the endpoint will take about 2 min to correctly initialize the Finder Extension functionality after enabling the extension or after the upgrade to 10.8 with an enabled extension.
- If you have a policy allowing management of the /Applications folder via the Copy Install Application filter, deleting multiple applications from the /Applications folder will result in a dialog prompting for administrator credentials. The workaround is to have your end-users delete applications one at a time.
- If you have enabled the Elevate Privilege Manager Agent Preference Pane (Sample) policy to elevate the Agent preference pane and you wish to target Big Sur, you will need to duplicate it and change the File Names to:

  `legacyLoader;legacyLoader-x86_64`
- If you have already duplicated the Elevate Privilege Manager Agent Preference Pane (Sample) policy to elevate the Agent preference pane and you wish to target Big Sur, you will need to change the File Names to:

  `legacyLoader;legacyLoader-x86_64`

10.8.1 Release Notes

October 8th, 2020:

Enhancements

Enhancements available with the 10.8.1 release of Privilege Manager. Enhancements are for both versions, On-premises and Cloud, unless otherwise outlined under a specific On-prem or Cloud subtopic.

- Improved the way we treat cookies as they pertain to IIS header limits (see https://docs.microsoft.com/en-us/troubleshoot/iis/http-bad-request-response-kerberos) in user group memberships to avoid potential error conditions.
- Group Member Based Approvals for offline support via Endpoint Group Member Approval Action.
  - Updates to the ServiceNow Integration Setup for supervisor roles based on group membership for ServiceNow integrations.
- Mobile and manual approvals now appear in the approval list in the Privilege Manager Console under **Tools | Manage Approvals**.
- Improved agent based Directory Services import for added computers.
- Improved applicable Application Control Configuration policy calculation to honor priority settings.

Cloud

- Privilege Manager now inventories domain users (full username, i.e. domain\username with SID) and groups in the Local Security Group Policy. Resource resolvers can use either to resolve to the unique resource for:
  - User Context Filter fields
  - GMA Action fields
  - Approval metadata reported during approval requests.

Bug Fixes

- The macOS agent can experience high memory utilization during File Inventory.
- 10.8.0 agent causes high CPU utilization.
- Unnecessary Change History records in DB that cause performance issues.
- Merge duplicate SID resources fails after on-prem AD sync.
- Changes to Syslog tasks can't be saved.
- XML entities in requests to ServiceNow would cause the request to fail.
- Database string reconfiguration does not work for integrated authentication.
- Promoting Windows domains to AD domains fails if the AD domain isn't available.
- The Application Justification Report by default shows all justification events for all computers instead of just events for the selected computer.
- Agent versions 10.4 and 10.5 cause error condition "Failed to resolve user SID" during approval workflow.
- RegEx syntax rules are broken when targeting secondary file filter information.
- When upgrading from 10.5 (and potentially other prior Privilege Manager versions), you may encounter an `Item Not Found` exception when first navigating to the console.
- Endpoints on Virtual Machines do not show local users associated with resources.
- In IE11 the dates in the agent log calendar view are rendered in the same color as the background and only readable when selected.
- When setting the **Monitor Resource** switch to active on a computer resource, an error is thrown.
- Custom Range in Console Log Viewer Only Displays Last Hour of Logs.
- The File Scan Results File Filter (Policy) shows the wrong description and references computers instead of a specific policy.
- Issue with using various VirusTotal and Cylance filters in different policies.
- In the Resource viewer the justification activity shows all justification events in the default "Application Justification Report".
- When setting the **Monitor Resource** switch to active on a computer resource, an error is thrown.
- Missing policy reports not working for all agents.
- After Upgrading to 10.8.0 AD Sync fails to run with "TypeError: Cannot read property 'Trigger' of null\n at active_directory".

Cloud

- Windows domain not promoted to AD domain after on-premises agent import.
- Sign out now working correctly.

macOS

- Scheduled commands are run later than their scheduled time due to the last run time timezone offset.
- Drag-n-drop app bundle from non-DMG can result in dialog asking for credentials.
- macOS Agent SecurityRatingFilterContract logic is inverted for the Failure and Timeout result.
- Predefined five XML entities in a policy name causes an exception when creating a ServiceNow approval request.

Known Issues

- Upgrading to Privilege Manager 10.8 causes a task to run to merge computer groups and remove unused system computer groups. This primarily affects the Application Control policies that are using resource targets/computer groups named **All Windows Computers with Application Control Agent Installed**. With 10.8, those policies will use the **Windows Computers** computer group and macOS will use **macOS Computers**.

  If you want to prevent this automatic merge, modify the XML of this item:

  `PrivilegeManager/#/item/xml/b2e02684-d154-48ca-9987-12b1759df822`

  Add on line 2 `<adc:Attributes>NoModify</adc:Attributes>`.
- Offline upgrades on **multiple** servers will need to be done manually.
- With an approval policy targeting a PowerShell script (.ps1 file) via secondary file filter, the Approval Notice pop-up causes a critical error alert when accessing the .ps1 file via right-click Edit menu option.

macOS Specific

- On endpoints using OneDrive, GoogleDrive, DropBox, or similar extensions, the endpoint will take about 2 min to correctly initialize the Finder Extension functionality after enabling the extension or after the upgrade to 10.8 with an enabled extension.

10.8.0 Release Notes

Enhancements

Enhancements available with the 10.8 release of Privilege Manager. Enhancements are for both versions, On-premises and Cloud, unless otherwise outlined under a specific On-prem or Cloud subtopic.

- New User Interface and User Experience.
  - New Policy Wizard driven Application Policy creation.
  - Resource Targets are now organized via "Local Security" on page 446.
  - Activation of Policies and Policy Priority changes available from the Application Policies overview page.
  - Dark theme support.
  - Refer to the Changelog for details about restructured documentation topics in alignment with the new UI.
- Enhanced upgrade process for on-premises instances. Privilege Manager now checks if updates are available and downloads details prior to proceeding. Refer to Updating Privilege Manager - Primary Node.

- The Application User Activity report provides audit details for user activities like logins and logouts. Refer to Application User Activity.
- The **Specific Installer Detection Filter** and **Generic Installer Detection Filter** are now labeled as legacy filters. These filters are only to be used to detect legacy installers that require the Windows Application Compatibility flag to be set.
- Support for multiple authentication providers, including multiple Active Directory domains, multiple Azure Active Directory domains, NTLM (on-premise), Secret Server, and Thycotic One authentication providers.
- Standard Privilege Manager users can be created to log into Privilege Manager in case a connected authentication provider is unavailable
- Additional metadata is included in Privilege Manager's approval workflow: SHA1 hash and commandline arguments
- Additional metadata is sent to ServiceNow for approval workflows: SHA1 hash, commandline arguments, company name, version
- User context filter supports local user and local group names match by text

macOS Specific Features

- Added macOS Agent Utility preference pane accessible via system preferences. Refer to macOS Agent Utility Preference Pane.
- Extended the **Agent Summary by OS** report to also contain macOS system serial number information.

Public API

Delinea introduces Privilege Manager's public API.

Cloud Specific Features

- Support Import of On-Prem Active Directory Users and Groups into Privilege Manager Cloud instances via Directory Services Agent (AD). Also refer to Bundled Install and Agent System Requirements.
- Integration with Delinea's SaaS based behavior analysis product, #PrivilegedBehaviorAnalytics (PBA), provides visibility into all processes interactively executed by end users.

Bugs Fixed

- Users in nested groups are not shown as child items when importing specific Azure AD users and groups.
- Adding a New AD Domain Uses the Wrong User Object (Not the One Selected).
- Hyperlink from approval email notification redirected URL from browser is not working in cloud environment.
- The task Import Specific Azure AD Users and Groups creates errors.
- Parent and child actions are processing messages wrong.
- SQL Lite Agent Errors with, 'Database is locked' on client item update.
- When the Dacpac triggers a change in the schema of the itemstate table, locking errors can occur.
- Resource Data Class Data will not be imported, if Data Class was just added during install.

- AD Domain Controller Resource synchronization issues.
- Missing Trigger after importing a Remote Scheduled Client Command.
- Cloning an Active Directory Foreign system configuration and creating a new AD does not remove previous settings (SID, DC, etc).
- Executable not being caught when using just the file hash for the filter.
- Agent registration fails due to foreign key constraint error pointing to missing target.
- The Resource Explorer does not honor an OU name update for Active Directory Foreign Systems.
- An URL specified with "http" only does not apply strict transport security for communication.
- Users in Privilege Manager Cloud are unable to configure tasks to send email reports.
- Domain user groups cannot be added to the User Context Filter.
- Secondary file filter pre-filtering performance is lacking.
- Errors when clicking on bar graphs for Local Security statistics about Users.
- Customer accounts with an ampersand (&) in the company name or license cannot activate their license.
- An error is thrown when attempting to add a managed user to a resource target.
- The Report Summary of Application Action report only contains the first 3 to 5 records when exported to CSV.
- When exporting a report with many records, the **Select All** option for CSV exports does not export all records.
- Upgrade banners are not displayed for the latest version.
- When creating or cloning an action, the user is unable to reference built-in or well-known local groups.
- CSV Report export adds apostrophe before - and + symbols
- When an endpoint is using Azure Service Bus to communicate with a Privilege Manager On-Prem instance, policies with a message, approval, or justification action do not appear and the application does not launch.
- An exception is thrown when attempting to sync after creating an SCCM connection.
- The subject line certificate filter does not match the certificate on file.
- No details available for the Codesign Entitled Elevated Application Filter.
- Issue using Multiple Security Groups in Computer Group not reflecting the correct number of computers.
- Active Directory Computer merge is not working correctly.
- Squishrunner.exe not working correctly with Delinea Application Control Agent installed.

macOS Specific

- System calculated due time for scheduled task as negative, causing an exception.
- macOS agents with a comma or equal sign in their name are not successfully registering.
- The approval/justification prompt appears twice for a policy elevating sudo commands.
- Slack's DMG application bundle is not correctly recognized as a finder copy candidate.

Agent Updates

- The agent is sending SHA1 and not SHA256 for Cylance integration.

Known Issues

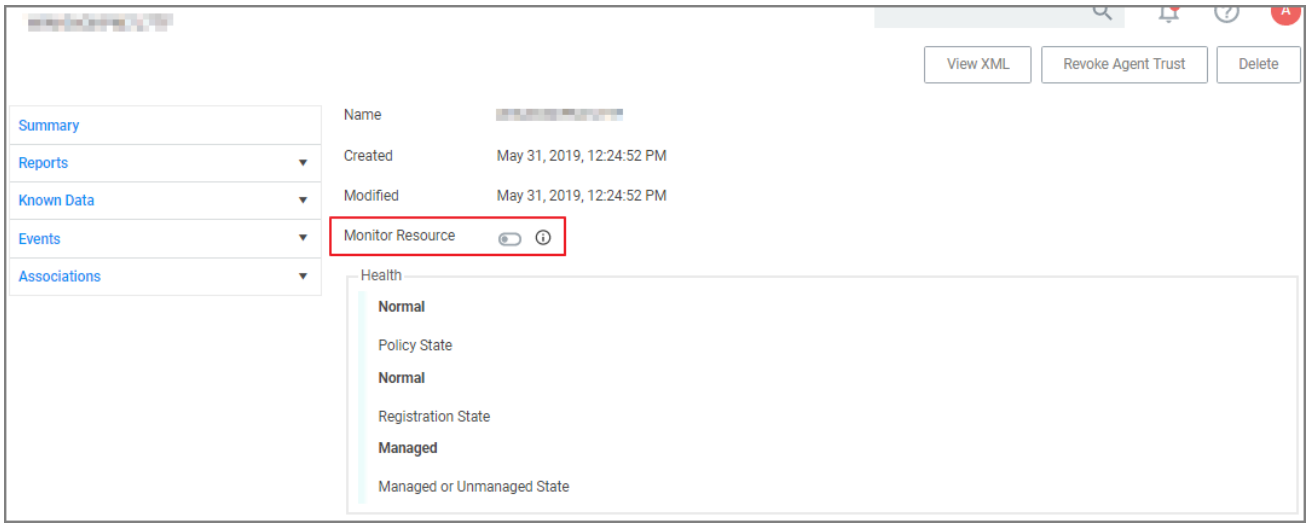
- Upgrading to Privilege Manager 10.8 causes a task to run to merge computer groups and remove unused system computer groups. This primarily affects the Application Control policies that are using resource targets/computer groups named **All Windows Computers with Application Control Agent Installed**. With 10.8, those policies will use the **Windows Computers** computer group and macOS will use **macOS Computers**.

  If you want to prevent this automatic merge, modify the XML of this item:

  `PrivilegeManager/#/item/xml/b2e02684-d154-48ca-9987-12b1759df822`

  Add on line 2 `<adc:Attributes>NoModify</adc:Attributes>`.

- When upgrading from 10.5 (and potentially other prior Privilege Manager versions), you may encounter an `Item Not Found` exception when first navigating to the console. The workaround for this is to recycle your app pools and then reload the console in your browser.
- When upgrading from 10.4 to the latest Privilege Manager version, the Admin menu might not load. The workaround for this is to recycle your app pools and then reload the console in your browser.
- When setting the **Monitor Resource** switch to active on a computer resource, an error is thrown.



- Offline upgrades on **multiple** servers will need to be done manually.
- The Directory Services Agent produced error messages about failed application control policy processing in the agent log.
- In IE11 the dates in the agent log calendar view are rendered in the same color as the background and only readable when selected.
- With an approval policy targeting a PowerShell script (.ps1 file) via secondary file filter, the Approval Notice pop-up causes a critical error alert when accessing the .ps1 file via right-click Edit menu option.

macOS Specific

- On endpoints using OneDrive, GoogleDrive, DropBox, or similar extensions, the endpoint will take about 2 min to correctly initialize the Finder Extension functionality after enabling the extension or after the upgrade to 10.8 with an enabled extension.

10.7.1 Release Notes

Release Date: Cloud 2020-03-05, On-premises 2020-03-12

Enhancements

Enhancements available with the 10.7.1 release of Privilege Manager. Enhancements are for both versions, On-premises and Cloud, unless otherwise outlined under a specific On-prem or Cloud subtopic.

- The Secret Server Vault integration does not require Secret Server to be set up as the authentication provider. Any supported authentication provider can be used, independent from using Secret Server as a Password Vault. Refer to Setting up Integration between Privilege Manager and Secret Server.
- Computers in Domain Groups can be leveraged as resource targets to be used in policies. Computer groups can be set up to utilize Active Directory security groups and organizational units (OUs). These so called domain security groups and OUs can be imported via Active Directory or Azure AD. However, OUs do not exist in Azure AD. Refer to "Local Security" on page 446.
- General in product user guidance improvement for Mobile Application configuration. Refer to Privilege Manager Mobile Application.
- The policy **Agent Service Start / Stop Control (Windows)** is now obsolete. Users should disable that policy and/or delete it. We have added a new policy named **Restrict Account Permissions on Agent Services (Windows)**. Users should clone that policy, to edit and assign to the desired targets, and enable. Refer to Agent Hardening
- Improved verbose logging during token validation logic.
- Report export options allow to select all data sets vs. data sets currently displayed on the page. Refer to Reports.
- On-premises only support for deployments with Amazon RDS database systems.

macOS Specific Features

- New Configuration Feed to ignore macOS Catalina Software Updates. For details refer to Ignoring macOS Updates.
- Best Practices for macOS system preference panes have been added, refer to "System Preferences" on page 155.
- Improved and new macOS event discovery filters, refer to "macOS Specific Filters" on page 738. Beginning with macOS Catalina, Apple changed the location of the application bundles that ship with the operating system. Traditionally, these applications were located in /Applications. Now they are located in /System/Applications. That location however is masked by Finder. The new and improved filters work with both locations.

- It is no longer necessary to include the **.app** extension for the Bundle Name property of an App Bundle Filter (e.g., Console.app). The agent will account for its presence while performing policy evaluation and properly match the filter if it is applicable. Refer to App Bundle Filter

Cloud Specific Features

- Data centers in Canada and Singapore have been added.
- Secret Server can be used as a password vault independent from the authentication provider.
- ServiceNow connector is automatically installed for all new cloud instances.
- The integrated SMTP server is automatically configured for all customers during the cloud instance setup, alleviating the need for customers to connect their own SMTP server.

Bug Fixes

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix. Bug Fixes are addressed for both versions On-premises and Cloud unless otherwise outlined under a specific On-prem or Cloud subtopic.

- Long lists of resource items are not scrollable when trying to view or select items. For example when adding a user to Local Security Groups or when looking at the password history of a user, the form cannot scroll down the entire list of users.
- The 10.7 agent fails and prevents execution on certain Java based applications.
- Reports exported to CSV only include information of the data currently displayed in the UI and not all data records from that report.
- Grids in reports are not properly sorting date column data.
- The offline approval picker is not displaying parameters and computer list does not fit into page.
- When editing an Import Directory or Import Directory Computers task, the Directory ID and the Query parameters cannot be saved.
- Secondary file filters are ignoring items with spaces in their name and not triggering appropriate policy actions.
- Exporting a FileParameterCollectionFilterContract does not export the underlying file resources.
- When creating Filters for Windows systems and the user has the Privilege Manager macOS Administrators role, an exception is shown.
- Misleading counts when built-in local Admin users are backed-up by provisioned user.
- When creating a copy of an **Approval Request (with ServiceNow Request Item Number) Form** action, the contents cannot be edited.
- Security ratings reports pagination is not working correctly.
- macOS latency in updating a VNODE structure on disk is resulting in application execution being denied.
- Cannot add new policies with application targets and enable.
- Selected credentials on AD foreign system cannot be edited.
- Changing authentication providers throws an exception.

- A Privilege Manager client license count is exceeded message is displayed when it exceeds the 90% threshold and valid licenses are still available.
- Any domain groups added as a local administrator in the LSS Computer Groups disappear after being added.
- Creating a user context filter with a properly formatted SID that does not exist fails. A malformed SID results in an unfriendly error message.
- Users cannot add new machines to a managed computer group.
- For policies using a Group Member Authenticated Message Action, members in nested groups are not validated during the authentication process.
- Users in nested groups don't get the proper application role.
- Cross site anti-forgery token validation was using an email as a match, but the value was configured as a name.
- The Resource Target Computer List removes previously selected items when attempting to add additional computers.
- Privilege Manager installs prior to 10.5 cannot be upgraded to 10.7.0.
- Preferences cannot be fetched or saved by non-administrative users.
- Agent hardening removes permissions to modify/delete Agent Services.
- ServiceNow connector fails when upgrading Privilege Manager from 10.4 to 10.7.0.
- The **Domain Users as Local Administrators** and **Summary of Domain Users as Local Administrators** reports are timing out when run in large environments.
- Changes to the default file inventory from the Event Discovery page are not saved.
- UNC share policies imported from Config Feeds are not displayed under policies.
- Application control agents installed on Windows 10 machines are not reported on the **Application Control Agent Summary** report.

Agent Updates

Refer to Software Downloads for the latest available agent software downloads.

Agent	Version	Bug Fixes
Core Delinea Agent	10.7.2266	Rebuild with bundle to include Application Control Agent updates.
Application Control Agent	10.7.2257	Secondary file filter pre-filtering performance is causing slowness when there are large numbers of child processes launched (such as git.exe for each file).
	10.7.2256	System experiencing poor performance for the Group Member Authenticated Messa ge Action.

Agent	Version	Bug Fixes
	10.7.2239	**Send SysLog ...** template based tasks to send logs to server fails.
	10.7.2219	Initial 10.7.1 release version.
Privilege Manager macOS Agent	10.7.30	Users are locked out of their macOS device user account and unable to log in again, if the option to reopen the application on next login is enabled.
	10.7.27	The download filter policy is not triggering due to invalid URL partial match logic.
		Local groups on macOS without a SID prevents local user inventory from completing.
		macOS agent experiences database contention when Office for macOS is installed or updated.
	10.7.21	Initial 10.7.1 release version.

Known Issues

- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Delinea recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.7 and newer macOS endpoint agent.
- When installing Privilege Manager on a Windows Server 2012 pointed to a DB that is running on SQL Server 2017 or above, SSDT binaries will need to be leveraged, which are only available in .NET 4.6 or above. If your Server 2012 has .NET 4.5.1, make sure to update it to the recommended .NET 4.6.1 version.

10.7 On-prem Release Notes

Release Date: 2019-12-09

Enhancements

Enhancements available with the 10.7 On-premises release of Privilege Manager:

- "Migrate Local Security Policies" on page 454 has been added. The migration path to the latest Local Security implementation provides an analysis report of issues like missing account credentials, or accounts that are not unique across targets, which can then be remediated before the migration.
- Change History auditing is available for resource items providing information on who initiated the change, at what date and time, and what type of change was made.
- The Remove Programs Utility in previous versions available via Configuration Feeds has been fully integrated with Privilege Manager Server and the Agents installation packages. The functionality has been expanded to also include Windows 10 App Store applications.
- Export and import of policies – including all dependent filter, action, and user context type items.

- A new Reset Licensing task was added.
- Support filtering on the subject name of a signed digital certificate allowing for much more generic certificate management.
- Dependency checks have been added to Privilege Manager for:
  - Deleting Items
  - Task Parameter and Schedule Parameters
- Agents Enhancements:
  - Agent Hardening
  - Agent will only receive new and updated policies that are relevant to that endpoint.
  - Enhance Client Item Cache Log View in Agent Utility.
- Support for configurable session and inactivity timeouts was added to the product.
- Allow right-click as a Delinea Admin for .msu and .msc files.
- ServiceNow ticket request numbers are displayed within Privilege Manager's prompts.
- Restrict access rights of File-Open dialogs that are launched from elevated processes.
- Domain User support in User Context Filters.
- When choosing a resource target, if an OU (Organizational Unit) is synced, the UI will display the computer and site names in their proper hierarchical structure
- When choosing a domain user for a Role, the picker now shows the domain and group membership of that user.
- Ability to bypass policy inspection during endpoint boot-up time in order to not affect boot-up time.
- Performance improvements during agent registration.
- Admin controlled list of extensions that are excluded from agent hashing.
- Application's friendly name displayed in approval workflow prompts.
- The default log size can be set using configuration settings in the administrative policies tab.
- The default permissions on the Application Control Agent Configuration Policies have been updated as follows:
  - TMS Admins and Windows Admins have read/write to the Application Control Agent Configuration Policy (Windows)
  - TMS Admins and Mac Admins have read/write to the Application Control Agent Configuration Policy (macOS)
  - TMS Admins, Windows Admins, and Mac Admins have Read/Create/Revoke access to Install codes
- macOS specific features:
  - Target specific commands on macOS using wildcards (starts with, ends with, contains) and regular expressions.
  - Secure Token support.
  - macOS discovery settings are more readily accessible on the discovery configuration page.

- PKG files can now directly be uploaded within the Privilege Manager UI, alleviating the need to first perform file inventory of those applications on the endpoints. The application policy manager has added ability to inventory a PKG file to allow building of policies prior to the discovery of the package.
- macOS Catalina support.

Bug Fixes

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix and specific details about the fix for some of the items.

- Changing the selected collection for an SCCM collection does not correctly update membership.
- Page goes blank when navigating to Admin | Configuration and "Enable Automatic Refresh of Privilege Manager Alerts in Browser" is disabled.
- Clear remote scheduled policy parameters when the command is changed.
- Message Action text editor in UI should support formatting included in XML.
- Double-clicking on column width adjustment in the Agent Log Viewer gives an Unhandled Exception.
- The Advanced Display Message Action is running in the background.
- New schedule updates do not display clearly in the schedule.
- The Application Justification Report returns no results.
- The Resource Monitor doesn't show counters after elevation.
- The COM Objects Elevation showing Windows UAC after canceling Delinea prompt.
- The “folder” view in the item selector does not work.
- The Event Counts on the Privilege Manager home are incorrect.
- Events are duplicated in the Event Discovery view.
- Win32Exe filter correctly handles files that have the internal attributes stripped.
- Remote/cloud connected clients that pull tasks are broken with service hardening tasks.
- The Password Age chart is broken and does not return any results.
- The Agent falls back to using legacy services and no longer retries to connect to current services.
- Offline Approval access is not available for the Privilege Manager HelpDesk User role.
- macOS Resource Targets are not updating when trying to add to a policy.
- On mouse-over the Statistics | Changes Period to Past Month report throws an exception.
- Changing an Azure User's Role membership in Azure is not reflected in Privilege Manager.
- An exception is thrown when navigating back to the Privilege Manager home after a session timeout.
- System does not handle logins to a machine without standard SIDs.
- The horizontal scrollbar is showing in the table for Windows Privilege Personas.
- The Policies table is congested when opened in smaller resolution.
- Reports displayed from the homepage may scroll pass the pagination controls.

- The Top Applications widget on the homepage throws an exception
- Several reports on the home page are not loading properly in Firefox.
- Updates to an exclusion filter name are not displayed after editing.
- The no licenses installed banner is missing.
- Redundant warnings appear about the anti-virus exclusion settings.
- An exception is thrown when navigating to the Foreign Systems tab on the Configuration page.
- AD synchronization does not work correctly for users with distinguished names in excess of 256 characters.
- The report generated from Purge Maintenance - Files Undiscovered has duplicate messages.
- The Agent configuration form does not show previous values when a user clicks cancel.
- Privilege Manager instances with Secret Server integration:
  - Secrets deleted from Secret Server create duplicate user credentials.
  - The expiration of a Secret Server session does not prevent access to Privilege Manager.
  - Changing Secret Server Role Permissions for Privilege Manager requires recycling TMS application pool.

Known Issues

- If you are upgrading from an older Privilege Manager version (pre 10.5) contact Delinea Support for assistance.
- Agent Hardening does not allow for an automated rollback. The workaround is to manually Restore Default Agent Permissions.
- If an issue is encountered with local UI preferences, Delinea recommends clearing the local storage cache to remove old preference values. This can be done by going to **Admin | Diagnostics** and clicking the **Clear Local Storage Cache** button.
- Creating copies of a Persona or currently selected task schedule does not work.
- The File Specification Filter definition does not work on macOS 10.15 (Catalina) when the File Names field starts with **com.apple.preference** and/or Path field starts with **/System/Library/PreferencePanes/**. Any Policies leveraging these filter definitions is also impacted.
- In Safari and Edge browsers column filtering for the Agent Policy State and Agent Policy State - Drilldown reports does not work.
- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Delinea recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.7 macOS endpoint agent.
- Privilege Manager macOS Administrator and Privilege Manager Windows Administrator roles:
  - If you are using the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles, you must also add those members to the Privilege Manager Users role or they may not be able to view some of the application filters or actions. If you are using Secret Server authentication, restarting the Privilege Manager app pools may be required to have this take effect.

- Members of the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles may not be able to delete some items such as policies, actions and filters, even though they are editable. Have a member of the Privilege Manager Administrators role delete those items if this occurs.

10.6 On-prem Release Notes

Release Date: 07/11/2019

Enhancements

Enhancements available with the 10.6 On-premises release of Privilege Manager include:

- The **Syslog integration** options have been improved and support for HTTP/HTTPS was added. The HTTPS option specifically supports integrations with DEVO. (Also available in Cloud release.)
- A **Getting Started dialog** provides information on initial configuration steps and links to documentation to guide customers through configuration, integration, and setup.
- An **Offline Approval Process** has been implemented so end users can request an approval for an application to continue to execute even if an endpoint is offline. Approval workflows usually require an endpoint to be online to send out the approval request and then receive an approval for an application to continue to run or execute. The offline approval dialog can be customized within the policy action configuration area. Summary reports for offline approvals are available via the Reports page in Privilege Manager.
- **Filters/Actions** have been added in support of various new Privilege Manager functionality:
  - Application Approval Request (with Offline Fallback) Message Action (Windows, macOS)
  - Copy Install Application (macOS)
  - User Requested Run As Administrator Filter (macOS)
  - Executable Declared as Privileged Filter (macOS)
  - Codesign Elevated Application Filter (macOS)
- **Direct approval process selection for ServiceNow** is now available in the Privilege Manager UI, and no longer requires SilverLight.
- The Windows agent supports the **display of the ServiceNow approval request ID** after the approval has been submitted.
- **Integration to use Azure AD as an authentication provider has been improved**. It is now possible to specify the Client ID and the Client Secret in the configuration for Azure AD. If not specified, the associated user credential will be used. This enables customers to use just one credential for both import and login, or use separate ones based on preference. Local Active Directory accounts can be imported and synchronized with Azure Active Directory. Tasks have been added to support importing a subset of the directory instead of needing to import the entire directory.
- **New macOS features**, refer to the macOS information under Platforms and Computer Groups for detailed information.

  - A policy can be created to allow or deny standard users to install specific applications by copying the application into the Applications folder.
  - Just as on Windows endpoints, users can request application self-elevation via a context menu action on macOS system endpoints. The application control is policy based and the macOS system with the endpoint agent must have been online at least once to request its policies from the Privilege Manager server.
- A setting was put in place to **cap the maximum number of events** that can be sent back to the server at 1 Million events. Once that threshold is reached, the oldest event is purged from the list. This setting can be adjusted in the Advanced section of the Configuration page.
- A **browser-based server Log Viewer** is now available from the Admin menu.
- **Error notification and performance in high latency environments** have been greatly improved in this release.
- **Bulk delete actions** have been added to support the removal of large numbers of file resources without timeouts.
- The Resource Targets on the Conditions tab of an ACS policy has been renamed to “when ANY match” for clarification of scope.
- General improvements to the Groups view within the Local Security area.
- The Privilege Manager feature to support RDP session monitoring is being discontinued.

Bug Fixes

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix and specific details about the fix for some of the items.

- In the Privilege Manager UI domain users cannot be added to TMS Roles, only groups may be added.
- When the URI information is deleted from an existing SMTP server configuration, the URI entry box disappears from the UI.
- The Privilege Manager UI does not correctly load policy details with large numbers of filters configured. Paging functionality has been added, defaulting to 10 items per page viewed. This can be customized on any given list page to a view of up to 100 items per page.
- Unable to edit configuration of "All Other Users and Groups" for groups in local security from “Ignore if found” to “Remove if found”. When this issue occurs, Privilege Manager will show an error, which then allows the user to fix the error by navigating to the “RemoteScheduledClientCommandContract” for the group that is having the issue, removing the input parameters for the provisioned group, and then retrying the change.
- Error upgrading to 10.5 U3 Directory Services for some specific conditions.
- LSS Member filter does not work if the number of members across endpoints and the number of endpoints is large.
- The Privilege Manager Remove Program Utility displays incorrect buttons for NoModify and NoRepair registry keys.
- The Add/Remove Programs Utility is preventing repairs to Microsoft Office products.
- The User Context Filter via SID Filter "create page" validation causes an error, which prevents the SID to be saved.

- After reboot, the endpoint agent creates a certificate based on the UUidCache information causing an invalid agentID error.
- A macOS account with a computed RelativeId (RID) that is null results in an exception that causes Local User Inventory to fail.
- macOS: The Administrator account (500) is required to be added to the managed Administrators (544) group.
- After editing a managed local group, the list of members will sometimes expand to include what appears to be the entire list of all users in the system. Refreshing the console will return to showing just the members that were configured.
- During Event Discovery, if the same file is discovered from 2 policies, only one file entry will be removed but receive an Acknowledge All. The second listing of the same file cannot be removed.
- Built-in Privilege Manager User does not have read access to policies.
- Privilege Manager relies on the Require Folders for SecretsSecret Server setting during integration set-up.
- Login button is displayed after authentication with Secret Server.
- Customer upgrading from version 8.x have issues deleting or saving items with GUID 71f3e19c-625c-4696-80e6-c9616554cb3c.
- UAC Override policy does not go into effect until UAC Override scheduled task is run.
- Event discovery resources stuck in Pending Assignment status.
- On macOS endpoints with agent version 10.6.19 installed, depending on the user interaction with the approval dialog, it is possible that after clicking Continue or Cancel the dialog is redisplayed and cannot be dismissed.

Known Issues

- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Delinea recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.6 macOS endpoint agent.
- If a customer implementation uses the Microsoft Azure Service Bus for their Internet connected clients, the clients will **NOT** be able to communicate with the Privilege Manager server after an upgrade to 10.6. Contact Delinea Support if you are using Microsoft Azure Service Bus and are planning to upgrade. This does not impact implementations using a Reverse Proxy.
- Privilege Manager macOS Administrator and Privilege Manager Windows Administrator roles:
  - If you are using the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles, you must also add those members to the Privilege Manager Users role or they may not be able to view some of the application filters or actions. If you are using Secret Serverauthentication, restarting the Privilege Manager app pools may be required to have this take effect.
  - Members of the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles may not be able to delete some items such as policies, actions and filters, even though they are editable. Have a member of the Privilege Manager Administrators role delete those items if this occurs.

10.6 Cloud Release Notes

Release Date: 05/30/2019

In this new release, Delinea expands its Enterprise-Grade Privileged Access Management (PAM) as a Service, offering Privilege Manager in the cloud and building upon its industry-leading cloud-ready solutions.

Enhancements

Enhancements available with the 10.6 Cloud release of Privilege Manager include:

- A Getting Started dialog provides information on initial configuration steps and links to documentation to guide customers through configuration, integration, and setup steps.
- An Offline Approval Process has been implemented so end users can request an approval for an application to continue to execute even if an endpoint is offline. Approval workflows usually require an endpoint to be online to send out the approval request and then receive an approval for an application to continue to run or execute. The offline approval dialog can be customized within the policy action configuration area. Summary reports for offline approvals are available via the Reports page in Privilege Manager.
- Clear communication for regularly scheduled or emergency maintenance tasks:
  - In Privilege Manager Cloud environments regularly scheduled maintenance tasks will be announced via a maintenance banner at least 14 days prior to the maintenance window being in effect.
  - Delinea will announce any regularly scheduled and emergency maintenance to inform customers when maintenance is performed on the cloud instance.
- Filters/Actions have been added in support of various new Privilege Manager functionality:
  - Application Approval Request (with Offline Fallback) Message Action (Windows, macOS)
  - Copy Install Application (macOS)
  - User Requested Run As Administrator Filter (macOS)
  - Executable Declared as Privileged Filter (macOS)
  - Codesign Elevated Application Filter (macOS)
- Direct approval process selection for ServiceNow is now available in the Privilege Manager UI, and no longer requires Silverlight.
- The Windows agent supports the display of the ServiceNow approval request ID after the approval has been submitted.
- Thycotic One is the access portal to Privilege Manager Cloud and provides data center access/support via Thycotic One US East, EU, and Australia Azure geo locations.
- Integration to use Azure AD as an authentication provider has been improved. It is now possible to specify the Client ID and the Client Secret in the configuration for Azure AD. If not specified, the associated user credential will be used. This enables customers to use just one credential for both import and login, or use separate ones based on preference. https://support.delinea.com/support/s/article/PM-How-to-Configure-Privilege-Manager-with-Secret-Server

Local Active Directory accounts can be imported and synchronized with Azure Active Directory. Tasks have been added to support importing a subset of the directory instead of needing to import the entire directory. https://support.delinea.com/support/s/article/PM-Setting-Up-Azure-Active-Directory-Sync

- macOS, refer to the Mac User Guide for detailed information on the new macOS features.
  - A policy can be created to allow or deny standard users to install specific applications by copying the application into the Applications folder.
  - Just as on Windows endpoints, users can request application self-elevation via a context menu action on macOS system endpoints. The application control is policy based and the macOS system with the endpoint agent must have been online at least once to request its policies from the Privilege Manager server.
- A policy was put in place to cap the maximum number of events that can be sent back to the server at 25000 events. Once the 25000 event comes in, the oldest event is purged from the list. For troubleshooting purposes this can be temporarily adjusted by Delinea support.
- A browser-based server Log Viewer is now available from the Admin menu.
- Error notification and performance in high latency environments have been greatly improved in this release.
- Bulk delete actions have been added to support the removal of large numbers of file resources without timeouts.
- The Resource Targets on the Conditions tab of an ACS policy has been renamed to “when ANY match” for clarification of scope.
- General improvements to the Groups view within the Local Security area.
- The Privilege Manager feature to support RDP session monitoring is being discontinued.

Bug Fixes

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix and specific details about the fix for some of the items

- In the Privilege Manager UI domain users cannot be added to TMS Roles, only groups may be added.
- When the URI information is deleted from an existing SMTP server configuration, the URI entry box disappears from the UI.
- The Privilege Manager UI does not correctly load policy details with large numbers of filters configured. Paging functionality has been added, defaulting to 10 items per page viewed. This can be customized on any given list page to a view of up to 100 items per page.
- Unable to edit configuration of "All Other Users and Groups" for groups in local security from “Ignore if found” to “Remove if found”. When this issue occurs, Privilege Manager will show an error, which then allows the user to fix the error by navigating to the “RemoteScheduledClientCommandContract” for the group that is having the issue and removing the input parameters for the provisioned group and then retry the change.
- Error upgrading to 10.5 U3 Directory Services for some specific conditions.
- LSS Member filter does not work if the number of members across endpoints and the number of endpoints is large.
- The Privilege Manager Remove Program Utility displays incorrect buttons for NoModify and NoRepair registry keys.
- The Add/Remove Programs Utility is preventing repairs to Microsoft Office products.

- The User Context Filter via SID Filter "create page" validation causes an error, which prevents the SID to be saved.
- After reboot, the endpoint agent creates a certificate based on the UUidCache information causing an invalid agentID error.
- A macOS account with a computed RelativeId (RID) that is null results in an exception that causes Local User Inventory to fail.
- macOS: The Administrator account (500) is required to be added to the managed Administrators (544) group.
- After editing a managed local group, the list of members will sometimes expand to include what appears to be the entire list of all users in the system. Refreshing the console will return to showing just the members that were configured.
- During Event Discovery, if the same file is discovered from 2 policies, only one file entry will be removed but receive an Acknowledge All. The second listing of the same file cannot be removed.
- Built-in Privilege Manager User does not have read access to policies.

Limitations in Privilege Manager Cloud 10.6 vs. On-prem

- The Local Active Directory features exists, but requires a direct connection to the domain controller, which is often not permissible due to firewall configurations.
- Secret Server integration for authentication and vaulting of local account credentials is not presently available.
- All license key management is done via Delinea and license keys are not visible on the licensing page. There are not presently options for customers to add additional licenses directly.
- Access to the Security Manager console (Silverlight version) is not available.
- Personas are not available.
- Server-side PowerShell scripts not signed by Delinea are not allowed. Custom server-side work can be done via Professional Services engagements.
- The setup is managed by Delinea and installations, upgrades, and repairs are unavailable to the customer directly, this includes setup, add/remove feature options, and connection option to existing Secret Server. Upgrade notices and banners are removed with upgrades being handled by Delinea during maintenance periods.

All other features and functionality of Privilege Manager On-premises and Cloud are the same.

Known Issues

- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Delinea recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.6 macOS endpoint agent.

10.5 and Previous Releases

10.5.4

Release Date: 12/11/2018

Enhancements

Listed below are the enhancements being provided in this release:

- When creating a resource target for a policy, the “Groups” option is available to allow targeting of organization units (OUs). See article: https://support.delinea.com/support/s/article/User-Defined-Resource-Targets-and-Collections
- A new report called “Server Node Status” will show the version installed on each server node in high availability environment. This report will inform customers of the installed version of Privilege Manager across multiple instances for high availability.

Bug Fixes

Listed below are the bugs that have been * Fixed in this release. (The product behavior is described as it was prior to the * Fix. In a few of the items below, the specific * Fix is also described.)

- Users with the Privilege Manager Helpdesk Users role are unable to approve items; get an error message.
- Authenticated XAML message does not work if agent cannot connect to domain. * Fix: When validating credentials, if the domain is not available Privilege Manager will now authenticate against the operating systems so that (if the domain isn't available) the agent will use the local database SAM cache.
- Purge Maintenance task times out on extremely large tables when performing a deletion of millions of records.
- Exporting the Application Summary Report to CSV fails.
- During upgrade, some servers don't have proper permissions to allow writing new certificates to C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys. * Fix: A new error message was added for Privilege Manager servers that do not have proper permissions during the upgrade to write new certificates to: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys.
- After successfully adding the first license, message saying “No records to display” is still displayed.
- Licensing page does not display an error if importing an invalid or duplicate license.
- On some reports, some valid filterable values are not being displayed as a selectable option after selecting the “Filter Report” button.
- Labels and information displayed when viewing a task does not properly align when the screen size is small.
- Option to “Backup the System” under “Client System Settings” policies does not elevate without selecting to apply to child processing. * Fix: Elevation will now occur automatically without having to change the child processing setting.
- Some Role membership group names are in all lowercase, not Pascal case.
- On the Help page, the link for the user guide is pointing to the Preferences page instead of the actual user guide.
- User is unable to press the ‘Cancel' button on the Preferences page.
- When the browser is made smaller, the page to create scheduled tasks has overlapping text.
- When editing a copy of the “Approval Request Form Action”, the selected value in the “Approval type” disappears when switching from view mode to edit mode.

- Changing the “Minimum Security Level” field in the console log settings is not limiting the records displayed in the logs.
- “Base URL” field for Privilege Manager server under Foreign systems reads as “Base URI”. * Fix: Text of the “Base URI” label in a Foreign System has been changed to “Base URL”.
- Selecting options besides the “Upper Case” option when configuring a user's password results in “Undefined” being displayed as a selected option.
- Incorrect error messages are displayed if a new User credential is saved without or with an incorrect password.
- After clicking “Import” on the Import Items page, the import button does not grey out to display feedback that the import is processing.
- Exception is thrown on “Client System Settings” page when the Assign Filter field is left blank.
- Assigning filters to any of the items in “Client System Settings” can cause the page to become unresponsive.
- On the Time of Day filter, changing the time under “Different Periods on Different Days” also incorrectly changes the times under “Same Period Every Day”.
- Clicking the Sort column of an empty report causes page to error.
- When deleting a filter or an action that is used in a policy, Privilege Manager correctly prevents the deletion but displays an incorrect error message.
- When building resource target queries, starting with “All Computers” causes poor performance. * Fix: This been removed from the default way resource target queries are built.
- “OU Directory Scope Collection Update” task fails if Collection.LastUpdated is null.
- Applications hang if a new certificate is created and the agent requests new client items before it updates applicable policies or registers with the server.
- Installing a new agent on a macOS endpoint results in a corrupted schedules.plist file.
- Azure AD tokens are expiring within minutes. * Fix: Azure AD will now last as long as normally issued tokens.
- If the “UNC Elevation Policy Template” Config Feed is imported, the "UNC Content Query" is erroring.
- When Secret Server and Privilege Manager are installed together using the combined installer, and a separate domain account without write permissions is used, subsequent upgrades fail if the domain account running the application pool does not have Write permissions on the TMS web folder.
- “Advanced Deny Notification Actions” are not included in dashboard counts and the list of denied files.

10.5.000003

Release Date: 9/25/2018

Bug Fixes

- Fixed issue where the macOS agent configuration did not have a default task check in interval saved.
- Fixed issue where queries for reports that are scoped to display only certain resources will fail if the Default Security Descriptor ID is null or empty.

- Fixed issue where large Active Directories caused the Collection and Resource Targeting Update task to run for too long.
- Fixed issue where Privilege Manager's authentication provider screen would crash if incorrectly configured. When Privilege Manager cannot reach an Active Directory domain, a useful error message is now displayed.
- Fixed issue where Privilege Manager task schedules are not properly saved and displayed.
- Fixed issue where the dashboard would display an unexpected error in a modal popup the state of a gauge undefined.
- Fixed issue where the sign-in page URL query string could be used to redirect a user to another URL by only allowing relative URLs.
- Fixed issue where Telerik grids were not able to be resized when zoomed in or out in Chrome, Firefox, and Edge.
- Fixed issue where the GetToken API returned an invalid token for unauthorized requests instead of a 401 response code.
- Fixed issue that allowed Privilege Manager to be embedded inside of an iframe.
- Fixed issue where a New Loaded Resource file is not assigned to an endpoint's agent after the Resource Discovery task is executed once.
- Fixed issue where the Resource Discovery task does not finish and will continue to display a spinner when discovering a New Loaded Resource file that is not assigned to an endpoint's agent.
- Fixed issue where a New Loaded Resource was not discoverable if the location has been discovered but the file has been removed from the endpoint.
- Fixed issue that displayed the HTTP status code instead of the actual server error when bad XML was imported to Privilege Manager.
- Fixed issue where the data grid within a policy that displays all the filters loads slowly.

macOS Agent Updates (version 10.5.12)

- Fixes issue where the macOS agent was not properly logging failed agent registration attempts when an invalid install code was used.
- Fixed issue where macOS agent was writing exceptions to the logs if v4 agent registration fails when connecting to a Privilege Manager version prior to 10.5.
- Fixed issues where initial basic inventory was not being removed after first running.

10.5.000001

Release Date: 9/04/2018

Bug Fixes

- Fixed issue where Privilege Manager, when configured with Secret Server for authentication, did not properly fall back to NTLM authentication if Secret Server was not properly configured.

- Fixed issue where Privilege Manager upgrade failed if duplicate IDs existed in [Ams].FileUploads or [Ams.Data].Win32_OperatingSystem tables.
- Fixed issue where Privilege Manager did not prevent deletion of an item referenced by another object. For example, it did not block a filter from being deleted if that filter was also being used by an active policy.
- Fixed an issue where the delete operation of computers did not properly display completion for long-running deletes.

10.5.000000

Release Date: 8/15/2018

Overview

Notable enhancements to 10.5 include a new dashboard as the home page, integration with Cylance reputation analysis, support for Azure Active Directory, performance enhancements, and improved agent security.

Important for Secret Server Combined Upgrades

If Secret Server is installed in conjunction with Privilege Manager, Secret Server must be upgraded to 10.5.000001 before you upgrade to Privilege Manager 10.5.000000.

10.5 Agent Upgrades

Unless the “Prevent Legacy Agent Registration (10.4 and older)” option is checked (Admin > Configuration > Advanced), older agent versions will still function in Privilege Manager 10.5.000000, but Delinea recommends that you do upgrade Privilege Manager agents to the 10.5 version due to security enhancements.

Note: That when installing new 10.5.000000 agents you will be prompted to install with a valid Install Code.

Enhancements

- New dashboard for deep reporting and visibility into the state of Privilege Manager.
- Integration with Cylance for real-time threat intelligence policy checks.
- Support for Azure Active Directory for authentication, resource targeting, and user context filters.
- Excel reports that are exported are sanitized to prevent macro injection attacks against end-users who open the Excel files.
- Cross site request forgery prevention implemented.
- Sensitive data encrypted on endpoint with machine, non-global key.
- Agent installation requires agent install code as a parameter or as a field entered when using the bundled installer for additional security.
- Redesign of agent/server trust requiring shared secret before agent can register with server and receive policies.
- Redesign of client item encryption to improve security.
- “Add new filter” and “Add to policy” buttons are on resource page for MSIs and scripts.

- Support for inventory filters added as secondary file filters to allow targeting of MSIs and scripts by hash.
- Support wildcards in fields of the Win32 executable filter. See inline help for details.
- Added SQL indexes for improved performance.
- Collection update and resource targeting update tasks are combined into task called “Run Policy Targeting Update.”
- Allow unattended uninstall of macOS agent by adding command-line option to suppress the user confirmation prompt.
- Reduced the time it takes a newly installed agent to download policies.
- Advanced message options for justification window supports end user authentication.
- Default to validating client item signatures on Windows agents.
- Support and maintenance license are viewable on the licenses page.
- Option to "Apply action to child processes" is unchecked by default.
- Deployment tab of a policy will display a button to update the collection of resource targets on demand.
- EULA not shown upon product upgrade.

Bug Fixes

- Fixed issue where Administrator group incorrectly displayed SYSTEM account as a member.
- Fixed issue where Server URL on agent was not updated if server was changed.
- Fixed issue where setting password rotation for a one-time update failed to rotate the password.
- Resolved error when custom approval process was initiated.
- Processed events are purged up from the [AMS.DATA].FileUploads, [AMS.DATA].FileUploadChunks, and [AMS.DATA].FileUploadSessions tables.
- Fixed issue where changed numeric values on the Advanced tab of the configuration page were not saved.
- Resolved schedule creation error in certain time zones.
- Resolved an issue where provisioning a local user would enable a disabled account and/or disable an enabled account.
- All internal links to support documentation now utilize https.

Known Issues

- If Secret Server is installed in conjunction with Privilege Manager,Secret Server must be upgraded to 10.5.000001 before you upgrade to Privilege Manager 10.5.000000.
- Agent trust is broken if VM UUID changes. Agent must be reinstalled to resolve.
- On the user screen in local security, the text “undefined” will appear if any option for password “Characters” is selected except 'Upper Case.'

10.4.001233

Release Date: 3/28/2018

Bug Fixes

- Resolved issue to ensure the trimming of the table storing data from uploaded files

10.4.001231

Release Date: 3/6/2018

Enhancements

- Support for SQL 2017
- Support for agent communication on Windows 7 systems with TLS 1.1 and SSL 3.0 disable
- Checks for a valid maintenance license to allow product upgrades
- Client item cache is cleared automatically
- Clicking the “Run” button for tasks indicates successful execution and prevents kicking off of multiple tasks
- Built-in administrator is prevented from being removed from group and the associated operation will display “Required Account”
- Support "log4net log (.log)" format in the Thycotic Monitor

Bug Fixes

- Reports on "Managed Local Users" and "Managed Local Group" will now allow users to select the account name as a drill through to a report on the computers the account exists on
- Breadcrumbs will display the correct name after renaming a computer group
- Upgrades will retain security ratings setting for VirusTotal
- Custom time of day filter correctly saves
- Simple policy view allows for new filter to be saved inline
- The popup allowing users to add a new account to a group allows sorting
- License correctly determines client and server types during basic inventory
- Ability to clone credentials has been removed when Privilege Manager stored credentials in Secret Server
- Resolved searching for filters from within the secondary file filter
- Upon saving group membership, the operation column correctly displays the action that will be taken on the associated account
- Resolved validation of password field for a managed user when using Edge browser
- Charts on the statistics page scale correctly for both small and large number of endpoints
- Resolved issue that prevented enabling of firewall policy
- Password scheduler saved when UTC is selected
- Allow domain groups to be members of roles

- Resolved issue preventing application inventory on network shares
- Prevent non administrative access to the Thycotic folder on local drive

10.4.000000

Release Date: 1/17/2018

Enhancements

- Least Privilege Enforcement for Local Users and Groups
- Provision local users and groups across all endpoints
- Permanently remove accounts from privileged local groups
- Prevent group membership from being changed directly on the endpoint, even by an administrator
- Local Account and Credential Management
- Uniformly apply user properties to local accounts
- Set secure and unique passwords for local accounts by defining character requirements and password length
- Rotate local account passwords automatically on a scheduled basis
- New and Enhanced User Interface
- Least Privilege features are built on top of a new easy to use and manage interface within the Local Security section of the application.
- Policies are easily deployed to groups of users or endpoints, making it easy to deploy least privilege in a phased approach
- Dashboard, reporting, and statistics are built into the interface to understand the current state of local users and groups on the endpoint and any changes. Easily spot vulnerabilities and trends.
- Actionable tips will appear inline when the environment is not following best practices
- Usability enhancements to application control functionality
- All grids have filtering options to narrow down large datasets
- Integration with Secret Server
- When using both Privilege Manager and Secret Server, passwords can be stored in Secret Server's vault
- Intended for use on endpoint workstations where remote management of local or non-domain accounts is not possible
- Secret Server enterprise PAM features can be used upon secrets that are managed by Privileged Manager
- Role Based Access
- Define users of the Privilege Manager application: set administrators, read only users, macOS users, Windows OS users, and helpdesk users
- Security trimmed access specifically designed for help desk users, who's responsibility it is to disclose passwords and approve/deny applications
- Reporting and Dashboards

- New reports provide visibility into local user and group membership, an audit of passwords that have been disclosed, a summary of local administrators, and all computers with passwords being managed by Privileged Manager
- Contextual reporting for each group of users and computers where least privilege policies are being applied to understand the affect of policies on users
- Simple charts provide an understanding of all endpoints with each individual user or group
- Dashboard will display trends of user's group membership changes, users being added and removed from groups, and passwords being disclosed. Trends provide insight into understanding outliers and potential rogue activity.
- Endpoint Visibility Utility
- Simple console deployed directly on the endpoint to check the communication status, register with the server, get the latest policies, view and export the logs.
- Ideal for enhanced visibility and understanding, especially when working directly with internal Delinea support or professional services.

Bug Fixes

- Language and text * Fixes on installer screens for non-English systems
- Issue where Privilege Manager's macOS copy helper would perform the copy without waiting the approval to complete. After * Fixing, we can now target .pkg files with policies.
- Secondary file filter will detect scripts being executed on Windows 10, after changes were made on how PowerShell scripts are launched on the OS
- Allow install (and pre-req install) to succeed if PowerShell Execution Policy is set to RemoteSigned in Group Policy
- Editing the Application Control Configuration policy will not set some values as blank
- Allow for configuration of "days" parameter for Purge Old Computers Task
- On macOS, track which certificate Privilege Manager received the most recent time it was registered.
- Ability to assign ServiceNow Process in Execute App Type through Privilege Manager UI

Known Issues

- On Windows 10 Enterprise edition with patch version 1709 (released October 26, 2017), UAC is not suppressed, and thus end users are prompted to enter admin credentials
- Unable to Clone Credential when Secret Server is used as vault
- Agent is not communicating to server on Windows 7 over TLS 1.1
- Creating a File Hash specific filter fails if there are spaces at the end of the hash

10.3.000014

Release Date: 8/29/2017

Enhancements

- Implemented automatic and continuous server-side logging
- Incorporated sandbox actions, allowing policies to limit the environments in which applications can execute
- On demand retrieval of a newly discovered file after event discovery. When “New Loaded Resource” is displayed, the user can click a new button called “Discover Now” to retrieve resources data.
- New check box added to the Event Discovery configuration to find all applications that require administrator rights to run

  ServiceNow configuration improvements
- Option to run the installation just for Secret Server, without installing Privilege Manager
- Upgrade of Privilege Manager will not require local admin rights when installed in conjunction with Secret Server
- Display warning if policy does not target any application
- Policy creation screen will remember simple or advanced view preference
- Paginate Resources list view
- Improved error handling on installation and the addition of an error icon indicating an issue
- Fixed issues in the VirusTotal reputation calculation and service call handling
- Upgrading a product within the setup app will also update dependent products
- Log files are now being stored to disk
- Installation Summary report now includes the last time agents registered
- Enhancements within installer for web applications to run as a user account
- Enhancements to better show report rows and chart sections that can be clicked into for drill-down into another report

Bug Fixes

- HTTP binding is not required on Privilege Manager website
- VirusTotal configuration is retained after upgrade or repair
- Issue installing the file inventory with machines using non-US date/time
- Trailing slash () will not affect the path field in Win32 and File Specification filters
- Future changes to agent configuration policies will be preserved and not overwritten
- All system policies are prevented from being edited so the user can create a copy

10.3.000000

Release Date: 7/12/2017

Enhancements

- Added an agent to allow deny and allow lists, approvals, and elevation on Macs.
- Added "easy Policies" to allow for simple ways of creating allow and deny lists.
- The dashboard is now a series of tiles designed to give a simpler experience.

10.2.000000

Release Date: 4/12/2017

Enhancements

- Updated Installer
- New installer to handle more prerequisites for HTTPS Bindings, WCF, and SQL
- Updated setup home for managing product upgrades going forward
- Session Monitoring Agents
- A new agent and policy is available to record RDP and console sessions. Note that this requires a Secret Server installation and licenses.
- For more information on RDP monitoring policies see this KB article

10.1.000000

Release Date: 1/18/2017

Enhancements

- Added page specific help into Privilege Manager console
- Added options in the Discovery for kicking off inventory tasks to expedite policy testing
- Brought EMET policy options into the Privilege Manager console
- Brought the Application Firewall policy options into the Privilege Manager console
- Added configuration feeds for uploading policies and other items from support.

Bug Fixes

- Fixed issue where adding a new Persona and going back to the persona home required a browser refresh to see the new Persona
- Fixed issues in IE where the Report title text on the report home was not a link.
- Fixed issues with configuring Active Directory domains.

Glossary

Action - An action is not required in a policy. A policy can be designed, for example, to simply listen for specific application activity, and provide auditing information back to Privilege Manager. However, to apply controls to a process (executable), one defines an action in the policy.

Some common actions include:

- Adjust process rights,
- Add administrative rights,
- Remove administrative rights,
- Deny application execution,
- Require user justification – user provides a reason why they need to run the application,
- Application warning,
- Bypass UAC prompt,
- Require workflow approval – user needs approval to run an application, etc.

Agent - An agent is installed on every endpoint in your network and will 1) Receive and apply defined policies to govern application/process execution on the endpoint, 2) Execute tasks on the endpoint and feed audit and inventory data back to Privilege Manager.

Agent BaseUrl - The agent must be set to communicate directly with Privilege Manager. There exists a registry entry that is set upon agent installation – this registry key is called BaseUrl.

Agent Registration – The Privilege Manager agent completes a registration process when it initially contacts Privilege Manager following installation, but also at regular configurable intervals. So, registration occurs regularly.

Arellia – Arellia was the original name for Privilege Manager. Because of this, many file paths and back end notations include the term Arellia or AMS instead of Privilege Manager or TMS.

Collection - A collection is a list of resources that meet a specific criteria, a query, list of names, etc.

Computer Groups – (also called Resource Targets) Specified sets of computers that meet certain criteria (e.g. type of operating system, location of the computer, etc) that are targeted by certain policies and scheduled tasks.

Condition – Policy Conditions contain one or more filters that defines what a policy is ‘listening' for. If the condition is satisfied in a policy, then an action is applied.

Config Feeds – Config Feeds can be found on the ADMIN page access from the Privilege Manager main page. Configuration feeds allow Delinea to deliver new components to Privilege Manager. Simply click through the options in the Config Feeds page starting with the Select Items button and download anything appropriate. Once the item is downloaded, it is immediately available in Privilege Manager.

Dashboard – Dashboard is the term for Privilege Manager's landing page, or Home screen.

Event – Any notable file data on your network that is targeted by Privilege Manager is called an Event.

Discovery – Discovery is a term used by Delinea for any information that is scanned or “found” on a network and imported or used by our products.

Least Privilege – Least Privilege is a security strategy organized around best practices. When effectively implemented, an organization's employees can navigate their network system with the lowest level of privileges. Higher credentials are flexibly (and often automatically) granted or denied based on users and the tasks being performed. This dynamic strategy significantly reduces the threat of security breaches across an organization without interfering with daily operations.

Filter – The Policy Condition lists one or more filters. A filter is defined to identify many things about an executable or process, or 'situation' when an executable or process is initiated.

Common Filters include:

- File specifications,
- Network location,
- Directory location,
- Application reputation,
- Application digital certificate,
- Time of day, User context (what AD security group a user belongs),
- Download source,
- Drive type,
- File owner,
- Internet Zone,
- Security Catalogs, etc.

Inclusion Filter/Exclusion Filter – When a filter is placed in the Inclusion Filters or Exclusion Filters under the Conditions tab of a policy definition, it can be used to explicitly include or exclude what is defined in the filter with respect to a policy. (I.e. Exclusion: apply this policy only if the user is NOT an administrator; Inclusion: apply this policy only if the computer is on the company network; Inclusion: apply this policy only to applications signed by a specific company's digital certificate, etc.).

Persona - Personas manage sets of privileges that are assigned to users on specific Windows computers or Computer Groups. A Persona includes a set of pre-defined filters and provide an easy way to assign policies based on Computer Groups and users. Filter parameters in a Persona are limited and specifically designed to be applied to Windows administrative users.

Policy – A set of conditions (Filters) that, when met, will apply an action to managed resources (target computers).

- **Blocking** – Type of policies that will deny an application from running based on a determined set of criteria.
- **Catch-All** Policy – A Catch-All policy is a type of Learning Mode policy that will gather information about any unknown events that happen in your network.
- **Elevation Policy** – An Elevation Policy will allow specified applications to run with administrator credentials.
- **Monitoring** – Monitoring is a dynamic method of managing applications that might not be included on a safelist or blocklist. Instead of trying to anticipate every executable users will run, you can apply a flexible policy that includes actions or reputation checking for unknown applications.
- **Non-Blocking** – Types of policies that will allow applications to run according to normal user credentials. This is often considered a neutral policy to specify trusted applications.

Policy Priority – Policies are evaluated in a certain order for each application that runs. If one policy blocks an application and ends execution before a second policy that was intended to elevate privileges, then only the block will occur. It is important to have an awareness of all policies that are defined and the order in which they are called by the agent.

RDP Monitor – Discontinued with version 10.6. The RDP Monitor is used to configure the Enhanced Session Monitoring feature in Secret Server. It is found in Privilege Manage because this feature uses the agent architecture defined by Privilege Manager, however this feature typically is not used in a Privilege Manager PoC.

Reputation Engine – Privilege Manager can call upon a reputation engine (e.g., VirusTotal) in real-time to check an application's public reputation. One can create a reputation checking policy in Privilege Manager through Monitoring policies. This type of policy can take application information and send it to the engine in real-time and act on the application based on the returned reputation. For example, if the reputation engine returns a BAD grade, the application can be denied. It is recommended to apply this type of policy to specific directories where new or unknown applications might reside – like the Downloads, TEMP, or Desktop directory.

Resource Targets – (also called Computer Groups) Specified sets of computers that meet certain criteria (e.g. type of operating system, location of the computer, etc) that are targeted by certain policies and scheduled tasks.

Scheduled Tasks – A Privilege Manager policy may be defined to be applied based on a schedule. These items run using the Task Scheduler on each endpoint, and are only accessible by Privilege Manager administrators.

Secret Server – Secret Server is a second Delinea product that many IT teams use to securely manage privileged accounts and passwords in an organization. Privilege Manager and Secret Server are separate products but often used together for a holistic approach to network security. The two products are highly integrated and some of the features cross between products. For example, the Secret Server license page houses Privilege Manager licenses.

Send Policy Feedback – Send Policy Feedback is a setting that can be enabled for any policy that sends information to Privilege Manager. This is used in Learning Mode Policies and often valuable during testing, configuration, or auditing projects.

Thycotic – Thycotic was a previous company name. To ensure backwards compatibility, some file paths and back end notations include the term Thycotic.

TMS – TMS is shorthand for Thycotic Management Server. It is an umbrella term for our base application layer that Privilege Manager runs on top of.

VirusTotal – The VirusTotal reputation service is supported by Privilege Manager as a reputation engine. A free VirusTotal API key will need to be obtained to use VirusTotal in Privilege Manager. Note that the free API has limits and may not be appropriate for a production environment that functions with over four requests per minute.